Oracle® Fusion Middleware

Upgrade Guide for Oracle Identity and Access Management

11*g* Release 2 (11.1.2.2.0)

E48646-09

February 2015

Documentation for Oracle Fusion Middleware administrators who wish to upgrade to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0).

ORACLE

Oracle Fusion Middleware Upgrade Guide for Oracle Identity and Access Management, 11*g* Release 2 (11.1.2.2.0)

E48646-09

Primary Author: Shynitha K S

Contributing Authors: Rajesh Gouthaman, Sreetama Ghosh

Contributors: Allison Sparshott, Arun Singla, Aruna Vempaty, Ashwini Singhvi, Astha Gupta, Ballaji Sahoo, Basavaraj Hungund, Bhavik Sankesara, Brad Donnison, Bruce Xie, Charles Wesley, Deepak Ramakrishnan, Derick Leo, Gaurav Johar, Gururaj B S, Kavita Tippanna, Kishor Negi, Kumar Dhanagopal, Lixin Zheng, Lokesh Gupta, Madhu Martin, Mark Karlstrand, Mark Wilcox, Mrudul Uchil, Nagasravani Akula, Neelanand Sharma, Neeraj Goel, Niranjan Ananthapadmanabha, Pallavi Rao, Peter Laquerre, Raminder Deep Kaler, Ramya Subramanya, Ravi Thirumalasetty, Rubis Chowallur, Sandeep Dongare, Sanjay Sadarangani, Sanjeev Sharma, Semyon Shulman, Shruthi Chikkanna, Sitaraman Swaminathan, Sree Chitturi, Srinivas Nagandla, Stephen Mathew, Steven Frehe, Stuart Duggan, Svetlana Kolomeyskaya, Tushar Wagh, Umesh Waghode, Vadim Lander, Vishal Mishra, Venu Shastri, William Cai, Wortimla Rs, , Yongqing Jiang

Contents

Preface xvii

Documentation Accessibility xvii
Related Documents xvii
Conventions xvii

Part I Understanding Oracle Identity and Access Management

1 Introduction to Oracle Identity and Access Management Upgrade

1.1 Oracle Identity and Access Management Overview 1-1
1.2 Upgrade Scenarios 1-2
1.3 Migration and Coexistence Scenarios 1-3
1.4 Supported Starting Points for Upgrade on Single Node 1-3
1.4.1 Supported Starting Points for Oracle Access Manager Upgrade 1-4
1.4.2 Supported Starting Points for Oracle Adaptive Access Manager Upgrade 1-4
1.4.3 Supported Starting Points for Oracle Identity Manager Upgrade 1-5
1.4.4 Supported Starting Points for Oracle Entitlements Server Upgrade 1-5
1.4.5 Supported Starting Points for Oracle Privileged Account Manager Upgrade 1-6
1.4.6 Supported Starting Points for Oracle Identity Navigator Upgrade 1-6
1.5 Supported Starting Points for Upgrading High Availability Environments 1-6
1.6 Documentation Roadmap 1-7

2 Common Upgrade Tasks

2.1 Reviewing System Requirements and Certification 2-1
2.2 Backing up the Existing Environment 2-2
2.3 Upgrading to Oracle WebLogic Server 10.3.6 2-2
2.4 Updating Oracle Identity and Access Management Binaries to 11*g* Release 2 (11.1.2.2.0) 2-2
2.4.1 Obtaining the Software 2-2
2.4.2 Starting the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Installer 2-3
2.4.3 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) 2-4
2.5 Creating Database Schemas Using Repository Creation Utility 2-4
2.5.1 Obtaining Repository Creation Utility 2-5
2.5.2 Starting Repository Creation Utility 2-5
2.5.3 Creating Schemas 2-5

2.6 Upgrading Schemas Using Patch Set Assistant ... 2-5
2.6.1 Checking Your Database and Schemas ... 2-5
2.6.2 Starting Patch Set Assistant ... 2-6
2.6.3 Using the Patch Set Assistant Graphical Interface to Upgrade Schemas ... 2-6
2.6.4 Verifying Schema Upgrade ... 2-7
2.7 Upgrading Oracle Platform Security Services ... 2-7
2.8 Stopping the Servers ... 2-10
2.8.1 Stopping the Managed Server(s) ... 2-11
2.8.2 Stopping the WebLogic Administration Server ... 2-12
2.8.3 Stopping the Node Manager ... 2-12
2.9 Starting the Servers ... 2-12
2.9.1 Starting the Node Manager ... 2-12
2.9.2 Starting the WebLogic Administration Server ... 2-12
2.9.3 Starting the Managed Server(s) ... 2-13

Part II Upgrading Oracle Identity and Access Management 11*g* Release 2 (11.1.2.x.x) Environments

3 Upgrading Oracle Access Manager 11*g* Release 2 (11.1.2.x.x) Environments

3.1 Upgrade Roadmap for Oracle Access Manager ... 3-2
3.2 Reviewing System Requirements and Certification ... 3-3
3.3 Shutting Down Administration Server and Access Manager Managed Server(s) ... 3-3
3.4 Backing Up Oracle Access Manager 11*g* Release 2 (11.1.2.x.x) Environment ... 3-3
3.5 Upgrading to Oracle WebLogic Server 10.3.6 ... 3-3
3.6 Upgrading Access Manager Binaries to 11.1.2.2.0 ... 3-3
3.7 Upgrading OAM and OPSS Schemas ... 3-4
3.8 Upgrading Oracle Platform Security Services ... 3-4
3.9 Copying Modified System mbean Configurations ... 3-4
3.10 Shutting Down Administration Server and Access Manager Managed Server(s) ... 3-5
3.11 Upgrading System Configuration ... 3-5
3.12 Starting Administration Server and Access Manager Managed Server(s) ... 3-6
3.13 Upgrading Oracle Access Management Mobile and Service ... 3-6
3.14 Verifying the Upgrade ... 3-7
3.15 Troubleshooting ... 3-7
3.15.1 Component Version Shows 11.1.1.5.0 After Upgrade ... 3-7

4 Upgrading Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.x.x) Environments

4.1 Upgrade Roadmap for Oracle Adaptive Access Manager ... 4-2
4.2 Reviewing System Requirements and Certification ... 4-2
4.3 Shutting Down Administration Server and Managed Servers ... 4-3
4.4 Backing Up Oracle Adaptive Access Manager 11.1.2.x.x ... 4-3
4.5 Optional: Upgrading Oracle WebLogic Server ... 4-3
4.6 Updating Oracle Adaptive Access Manager Binaries to 11.1.2.2.0 ... 4-3
4.7 Upgrading OAAM, MDS, IAU, and OPSS Schemas ... 4-3
4.8 Upgrading Oracle Platform Security Services ... 4-4

4.9 Starting the Servers ... 4-4
4.10 Redeploying the Applications ... 4-4
4.11 Verifying the Upgrade ... 4-6

5 Upgrading Oracle Identity Manager 11*g* Release 2 (11.1.2.x.x) Environments

5.1 Upgrade Roadmap for Oracle Identity Manager ... 5-1
5.2 Pre-Upgrade Steps ... 5-3
5.2.1 Feature Comparison ... 5-3
5.2.2 Reviewing System Requirements and Certification ... 5-6
5.2.3 Generating and Analyzing the Pre-Upgrade Report ... 5-6
5.2.3.1 Obtaining Pre-Upgrade Report Utility ... 5-6
5.2.3.2 Generating the Pre-Upgrade Report ... 5-6
5.2.3.3 Analyzing the Pre-Upgrade Report ... 5-9
5.2.4 Backing Up Oracle Identity Manager 11.1.2.x.x Environment ... 5-19
5.2.5 Setting JVM Properties for Oracle Identity Manager Server(s) ... 5-19
5.2.6 Shutting Down Node Manager, Administration Server and Managed Server(s) ... 5-20
5.3 Upgrading the Oracle Home and Database Schemas ... 5-21
5.3.1 Upgrading Oracle WebLogic Server to 10.3.6 ... 5-21
5.3.2 Upgrading Oracle SOA Suite to 11.1.1.7.0 ... 5-21
5.3.3 Upgrading Oracle Identity Manager Binaries to 11.1.2.2.0 ... 5-22
5.3.4 Upgrading Schemas ... 5-23
5.3.5 Upgrading Oracle Platform Security Services ... 5-23
5.3.6 Upgrading Java Required Files (JRF) ... 5-24
5.4 Upgrading the Oracle Identity Manager Middle Tier ... 5-24
5.4.1 Starting Administration Server and SOA Managed Server(s) ... 5-25
5.4.2 Upgrading Oracle Identity Manager Middle Tier ... 5-25
5.4.2.1 Additional Task for Windows 64-Bit Users Before Upgrading Middle Tier ... 5-25
5.4.2.2 Upgrading the Oracle Identity Manager Middle Tier ... 5-25
5.4.2.3 Verifying the Middle Tier Upgrade ... 5-28
5.4.3 Restarting all the Servers ... 5-28
5.5 Upgrading Other Oracle Identity Manager Installed Components ... 5-28
5.5.1 Upgrading Oracle Identity Manager Design Console ... 5-28
5.5.2 Upgrading Oracle Identity Manager Remote Manager ... 5-30
5.6 Post-Upgrade Steps ... 5-30
5.6.1 Performing the Post-Upgrade Tasks ... 5-30
5.6.1.1 Reviewing Performance Tuning Recommendations ... 5-31
5.6.1.2 Upgrading Request Data ... 5-31
5.6.1.3 Configuring BI Publisher Reports ... 5-32
5.6.1.4 Targeting JRFWSAsyncJmsModule to Oracle Identity Manager Server ... 5-32
5.6.1.5 Creating PeopleSoft Enterprise HRMS Reconciliation Profile ... 5-33
5.6.1.6 Reviewing OIM Data Purge Job Parameters ... 5-33
5.6.1.7 Reconfiguring Lookup Based UDF Field ... 5-33
5.6.1.8 Reviewing Connector Certification ... 5-34
5.6.1.9 Verifying the Functionality of Connectors ... 5-35
5.6.2 Verifying the Upgrade ... 5-35

6 Upgrading Oracle Entitlements Server 11*g* Release 2 (11.1.2.x.x) Environments

6.1 Upgrading Oracle Entitlements Server 11.1.2.x.x Administration Server 6-1
6.1.1 Upgrade Roadmap for Oracle Entitlements Server Administration Server 6-2
6.1.2 Reviewing System Requirements and Certification 6-2
6.1.3 Shutting Down Administration Server and Oracle Entitlements Server Managed Servers 6-3
6.1.4 Upgrading Oracle WebLogic Server (If Necessary) 6-3
6.1.5 Updating Oracle Entitlements Server Binaries to 11.1.2.2.0 6-3
6.1.6 Upgrading Oracle Platform Security Services Schema 6-3
6.1.7 Upgrading Oracle Platform Security Services 6-4
6.1.8 Deleting Certain Directories From the Domain 6-4
6.1.9 Starting the Administration Server and the Managed Servers 6-4
6.1.10 Verifying the Oracle Entitlements Server Administration Server Upgrade 6-4
6.2 Upgrading Oracle Entitlements Server 11.1.2.x.x Client 6-5
6.2.1 Upgrade Roadmap for Oracle Entitlements Server Client 6-5
6.2.2 Stopping all Security Module Instances 6-5
6.2.3 Upgrade Oracle Entitlements Server Client to 11.1.2.2.0 6-5
6.2.3.1 Prerequisites 6-6
6.2.3.2 Obtaining the Software 6-6
6.2.3.3 Installing Oracle Entitlements Server Client 11*g* Release 2 (11.1.2.2.0) 6-6
6.2.3.4 Verifying the Installation 6-6
6.2.4 Starting the Security Modules 6-6
6.2.5 Verifying Oracle Entitlements Server Client Upgrade 6-6

7 Upgrading Oracle Privileged Account Manager 11*g* Release 2 (11.1.2.x.x) Environments

7.1 Upgrade Roadmap for Oracle Privileged Account Manager 7-2
7.2 Reviewing System Requirements and Certification 7-3
7.3 Exporting the Pre-Upgrade Data 7-3
7.4 Stopping the Administration Servers and the Managed Server(s) 7-4
7.5 Upgrading Oracle WebLogic Server to 10.3.6 7-5
7.6 Updating Oracle Privileged Account Manager Binaries to 11.1.2.2.0 7-5
7.7 Upgrading the Database Schemas 7-5
7.8 Start the Administration Server and the Managed Server(s) 7-5
7.9 Redeploying the Applications 7-5
7.9.1 Redeploying Oracle Identity Navigator Application 7-6
7.9.2 Redeployng Oracle Privileged Account Manager Application 7-7
7.10 Enabling TDE or Non-TDE Mode in OPAM Data Store 7-8
7.10.1 Configuring TDE Mode in Data Store 7-9
7.10.1.1 Enabling TDE in the Database 7-9
7.10.1.2 Enabling Encryption in OPAM Schema 7-9
7.10.2 Configuring Non-TDE Mode in Data Store 7-9
7.11 Importing the Pre-Upgrade Data 7-10
7.12 Clearing Pre-Upgrade OPSS Artifacts 7-10
7.13 Optional: Configuring the Oracle Privileged Account Manager 11.1.2.2.0 Session Manager . 7-11

7.14 Optional: Configuring Oracle Identity Navigator Application on OPAM Managed Server .. 7-11
7.15 Verifying the Oracle Privileged Account Manager Upgrade 7-11

8 Upgrading Oracle Identity Navigator 11*g* Release 2 (11.1.2.x.x) Environments

8.1 Upgrade Roadmap for Oracle Identity Navigator 8-2
8.2 Reviewing System Requirements and Certification 8-3
8.3 Exporting Oracle Identity Navigator 11.1.2.x.x Metadata 8-3
8.4 Shutting Down Administration Server and Managed Servers 8-4
8.5 Upgrading Oracle WebLogic Server to 10.3.6 8-4
8.6 Updating Oracle Identity Navigator Binaries to 11.1.2.2.0 8-4
8.7 Creating Oracle Platform Security Services Schema 8-4
8.8 Extending Oracle Identity Navigator 11.1.2.x.x Component Domains with Oracle Platform Security Services Template 8-4
8.9 Upgrading Oracle Platform Security Services 8-5
8.10 Configuring Database Security Store 8-5
8.11 Starting the WebLogic Administration Server 8-6
8.12 Verifying the Deployment Summary 8-6
8.13 Upgrading Oracle Identity Navigator Application 8-6
8.14 Importing the Oracle Identity Navigator 11.1.2.2.0 Metadata 8-7
8.15 Verifying the Upgrade 8-8
8.16 Optional: Configuring Oracle Identity Manager on the Oracle Privileged Account Manager Managed Server from the Administration Server 8-9

Part III Upgrading Oracle Identity and Access Management 11*g* Release 1 (11.1.1.x.x) and 9.x Environments

9 Upgrading Oracle Access Manager 11*g* Release 1 (11.1.1.x.x) Environments

9.1 Upgrade Roadmap for Oracle Access Manager 9-2
9.2 Reviewing System Requirements and Certification 9-3
9.3 Shutting Down Administration Server and Managed Servers 9-3
9.4 Backing Up Oracle Access Manager 11g Release 1 (11.1.1.x.x) 9-3
9.5 Upgrading Oracle WebLogic Server 9-3
9.6 Creating Oracle Access Management Access Manager Schemas Using Repository Creation Utility 9-4
9.7 Upgrading Oracle Access Manager Binaries to 11.1.2.2.0 9-4
9.8 Extending Oracle Access Manager 11.1.1.x.x Component Domains with Oracle Platform Security Services Template 9-4
9.9 Upgrading Oracle Platform Security Services Schemas 9-5
9.10 Upgrading Oracle Platform Security Services 9-6
9.11 Configuring Oracle Platform Security ServicesSecurity Store 9-6
9.12 Exporting Access Data 9-6
9.13 Importing Access Data 9-11
9.14 Copying Modified System mbean Configurations 9-13
9.15 Starting the Administration Server and Access Manager Managed Servers 9-14
9.16 Redeploying Oracle Access Management Access Manager Servers and Shared Libraries 9-14

9.17 Stopping the Administration Server and Access Manager Managed Servers 9-17
9.18 Deleting Folders 9-17
9.19 Upgrading System Configuration 9-17
9.20 Starting the Administration Server and Access Manager Managed Servers 9-18
9.21 Verifying the Upgrade 9-18
9.22 Troubleshooting 9-19
9.22.1 Exception While Running ImportAccessData Command 9-19
9.22.2 Exception While Deploying Application 9-19
9.22.3 Exception While Restarting Administration Server 9-20
9.22.4 Exception While Restarting Managed Server 9-21
9.22.5 Component Version Shows 11.1.1.5.0 After Upgrade 9-21

10 Upgrading Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.x.x) Environments

10.1 Upgrade Roadmap for Oracle Adaptive Access Manager 10-2
10.2 Reviewing System Requirements and Certification 10-2
10.3 Shutting Down Administration Server and Managed Servers 10-3
10.4 Backing Up Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x) 10-3
10.5 Optional: Upgrading Oracle WebLogic Server 10-3
10.6 Upgrading Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.2.0) 10-3
10.7 Upgrading OAAM, MDS, IAU, and OPSS Schemas 10-4
10.8 Extending Oracle Adaptive Access Manager 11.1.1.x.x Component Domains with OPSS Template 10-4
10.9 Upgrading Oracle Platform Security Services 10-5
10.10 Configuring OPSS Security Store 10-5
10.11 Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers 10-6
10.12 Redeploying the Applications 10-6
10.13 Deleting Folders 10-8
10.14 Restarting the Servers 10-9
10.15 Verifying the Upgrade 10-9

11 Upgrading Oracle Identity Manager 11*g* Release 1 (11.1.1.x.x) Environments

11.1 Upgrade Roadmap for Oracle Identity Manager 11-1
11.2 Pre-Upgrade 11-4
11.2.1 Feature Comparison 11-4
11.2.2 Reviewing System Requirements and Certification 11-7
11.2.3 Generating and Analyzing the Pre-Upgrade Report 11-7
11.2.3.1 Obtaining Pre-Upgrade Report Utility 11-8
11.2.3.2 Generating the Pre-Upgrade Report 11-8
11.2.3.3 Analyzing Pre-Upgrade Report 11-10
11.2.4 Ensuring That getPlatformTransactionManager() Method is Not Used in Custom Code 11-20
11.2.5 Emptying the oimProcessQueue JMS Queue 11-20
11.2.6 Other Prerequisites 11-20
11.2.7 Ensuring That JRF is Upgraded 11-21
11.2.8 Creating Reconciliation Field of Type IT Resource 11-22

11.2.9 Backing Up Oracle Identity Manager 11g Release 1 (11.1.1.x.x) 11-23
11.2.10 Setting JVM Properties for Oracle Identity Manager Server(s) 11-23
11.2.11 Shutting Down Node Manager, Administration Server and Managed Servers ... 11-24
11.3 Upgrade Procedure 11-24
11.3.1 Upgrading Oracle WebLogic Server 11-25
11.3.2 Upgrading Oracle SOA Suite to 11.1.1.7.0 11-25
11.3.3 Upgrading Oracle Identity Manager Binaries to 11.1.2.2.0 11-26
11.3.4 Creating Oracle Platform Security Services Schema 11-27
11.3.5 Upgrading Oracle Platform Security Services Schemas 11-28
11.3.6 Extending Oracle Identity Manager 11.1.1.x.x Component Domains with OPSS Template 11-28
11.3.7 Upgrading Oracle Platform Security Services 11-29
11.3.8 Configuring OPSS Security Store 11-29
11.3.9 Upgrading Oracle Identity Management Schemas Using Patch Set Assistant 11-30
11.3.9.1 Version Numbers After Upgrading Schemas 11-30
11.3.10 Starting the Administration Server and SOA Managed Server 11-30
11.3.11 Upgrading Oracle Identity Manager Middle Tier 11-31
11.3.12 Verifying Oracle Identity Manager Middle Tier Upgrade 11-33
11.3.13 Changing the Deployment Order of Oracle Identity Manager EAR 11-36
11.3.14 Restarting the Administration Server and SOA Managed Server 11-36
11.3.15 Patching Oracle Identity Management MDS Metadata 11-38
11.3.16 Upgrading Oracle Identity Manager Design Console 11-39
11.3.17 Upgrading Oracle Identity Manager Remote Manager 11-40
11.3.18 Configuring Oracle BI Publisher 11.1.1.7.1 11-40
11.3.19 Deploying Oracle Identity Manager BI Publisher Reports 11-41
11.4 Post-Upgrade Steps 11-41
11.4.1 After You Upgrade 11-42
11.4.2 Validating the Database Objects 11-43
11.4.3 Creating sysadmin Key 11-43
11.4.4 Impact of Removing Approver-Only Attribute in Request Data Set 11-43
11.4.5 Changes to Request API After Upgrading to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0) 11-45
11.4.5.1 API Methods Deprecated in RequestService 11-46
11.4.5.2 API Methods Deprecated in UnauthenticatedRequestService 11-46
11.4.5.3 SELF Request Types Deprecated 11-46
11.4.5.4 API Methods That Have Changed in Terms of Usage 11-47
11.4.6 Enabling Oracle Identity Manager-Oracle Access Manager Integration After Upgrading to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0) 11-50
11.4.6.1 Using 10*g* WebGate for Oracle Identity Manager-Oracle Access Manager Integration 11-51
11.4.6.2 Using 11*g* WebGate for Oracle Identity Manager-Oracle Access Manager Integration 11-51
11.4.7 Running the Entitlement List Schedule 11-52
11.4.8 Running the Evaluate User Policies Scheduled Task 11-52
11.4.9 Running Catalog Synchronization 11-53
11.4.10 UMS Notification Provider 11-53
11.4.11 Upgrading User UDF 11-55
11.4.11.1 Rendering the UDFs 11-55

11.4.11.2 User Interface Customization for 11.1.1.x.x Mandatory UDF and OOTB Attributes. 11-57
11.4.11.3 Lookup Query Modification 11-58
11.4.12 Upgrading Application Instances 11-58
11.4.13 Redeploying XIMDD 11-59
11.4.14 Redeploying SPML-DSML 11-60
11.4.15 Customizing Event Handlers 11-60
11.4.16 Upgrading SOA Composites 11-61
11.4.16.1 OOTB Composites Not Modified Before Upgrading 11-61
11.4.16.2 OOTB Composites Modified Before Upgrading And Custom Composites ... 11-62
11.4.17 Provisioning Oracle Identity Management Login Modules Under WebLogic Server Library Directory 11-63
11.4.18 Reviewing Performance Tuning Recommendations 11-64
11.4.19 Authorization Policy Changes 11-64
11.4.20 Creating Password Policies 11-65
11.4.21 Creating PeopleSoft Enterprise HRMS Reconciliation Profile 11-66
11.4.22 Reviewing OIM Data Purge Job Parameters 11-66
11.4.23 Migrating Customized Oracle Identity Manager Reports 11-66
11.4.24 Reviewing Connector Certification 11-66
11.4.25 Verifying the Functionality of Connectors 11-67
11.4.26 Updating the Provider URL For ForeignJNDIProvider-SOA 11-67
11.4.27 Verifying the Upgrade 11-67
11.5 Troubleshooting 11-68
11.5.1 Oracle Identity Manager Upgrade Control Points 11-70

12 Upgrading Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) Environment

12.1 Upgrading Oracle Entitlements Server Administration Server 12-1
12.1.1 Upgrade Roadmap for Oracle Entitlements Server Administration Server 12-2
12.1.2 Reviewing System Requirements and Certification 12-2
12.1.3 Shutting Down Administration Server and Managed Servers 12-3
12.1.4 Backing Up Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) 12-3
12.1.5 Optional: Upgrading Oracle WebLogic Server 12-3
12.1.6 Upgrading Oracle Entitlements Server Administration Server 11*g* Release 2 (11.1.2.2.0) 12-3
12.1.7 Creating Oracle Platform Security Service Schema 12-4
12.1.8 Upgrading Oracle Platform Security Services Schema 12-4
12.1.9 Executing R2_Upgrade.sql 12-5
12.1.10 Creating New Oracle Entitlements Server Domain 12-5
12.1.11 Exporting Encryption Key 12-5
12.1.12 Re-Associating Policy Stores 12-6
12.1.12.1 Policy Store is DB 12-6
12.1.12.2 Policy Store is OID 12-8
12.1.13 Upgrading Oracle Platform Security Services 12-10
12.1.14 Starting the Administration Server and Oracle Entitlements Server Managed Servers ... 12-10
12.1.15 Redeploying APM 12-10
12.1.16 Verifying the Upgrade 12-11

12.2 Upgrading Oracle Entitlements Server Client Server 12-11
12.2.1 Upgrade Roadmap for Oracle Entitlements Server Client Server 12-12
12.2.2 Stopping all Security Module Instances 12-12
12.2.3 Upgrading Oracle Entitlements Server Client 11*g* Release 2 (11.1.2.2.0) 12-12
12.2.3.1 Prerequisites 12-13
12.2.3.2 Obtaining the Software 12-13
12.2.3.3 Installing Oracle Entitlements Server Client Server 11*g* Release 2 (11.1.2.2.0) 12-13
12.2.3.4 Verifying the Installation 12-13
12.2.4 Changing Username and Password for the New Schemas 12-13
12.2.5 Starting the Security Modules 12-15
12.2.6 Verifying the Upgrade 12-15

13 Upgrading Oracle Identity Navigator 11*g* Release 1 (11.1.1.x.x) Environments

13.1 Upgrade Roadmap for Oracle Identity Navigator 13-2
13.2 Reviewing System Requirements and Certification 13-3
13.3 Exporting Oracle Identity Navigator 11.1.1.x.x Metadata 13-3
13.4 Shutting Down Administration Server and Managed Servers 13-4
13.5 Optional: Upgrading Oracle WebLogic Server 13-4
13.6 Upgrading Oracle Identity Navigator 11*g* Release 2 (11.1.2.2.0) 13-4
13.7 Creating Oracle Platform Security Services Schema 13-4
13.8 Extending Oracle Identity Navigator 11.1.1.x.x Component Domains with Oracle Platform Security Services Template 13-4
13.9 Upgrading Oracle Platform Security Services 13-5
13.10 Configuring Oracle Platform Security Services Security Store 13-5
13.11 Starting the Administration Server 13-6
13.12 Verifying the Deployment Summary 13-6
13.13 Upgrading Oracle Identity Navigator Application 13-6
13.14 Importing the Oracle Identity Navigator 11.1.2.2.0 Metadata 13-7
13.15 Verifying the Upgrade 13-8
13.16 Optional: Configuring Oracle Identity Navigator on OPAM Managed Server 13-9

14 Upgrading Oracle Identity Manager 9.1.x.x Environments

14.1 Upgrade Roadmap for Oracle Identity Manager 14-1
14.2 Pre-Upgrade Steps 14-3
14.2.1 Feature Comparison 14-4
14.2.2 Reviewing System Requirements and Certification 14-8
14.2.3 Backing Up Database Used by Oracle Identity Manager 9.1.x.x 14-8
14.2.4 Generating and Analyzing the Pre-Upgrade Report 14-8
14.2.4.1 Obtaining Pre-Upgrade Report Utility 14-9
14.2.4.2 Generating the Pre-Upgrade Report 14-9
14.2.4.3 Analyzing the Pre-Upgrade Report 14-11
14.2.5 Upgrading the OSI Data 14-17
14.2.6 Validating xlconfig.xml File 14-17
14.2.7 Creating Reconciliation Field of Type IT Resource 14-17
14.3 Installing New Oracle Home and Upgrading Database Schemas 14-18
14.3.1 Creating the Necessary Schemas 14-18

14.3.2 Installing Oracle WebLogic Server 10.3.6 ... 14-19
14.3.3 Installing Oracle SOA Suite 11.1.1.7.0 and Applying Mandatory SOA Patches ... 14-19
14.3.4 Installing Oracle Identity Manager 11.1.2.2.0 ... 14-19
14.3.5 Upgrading Oracle Identity Manager Schema ... 14-19
14.3.6 Upgrading Oracle Platform Security Services Schema ... 14-21
14.3.7 Creating a Domain for Oracle Identity Manager 11.1.2.2.0 ... 14-21
14.3.8 Configuring Database Security Store ... 14-21
14.3.9 Starting Administration Server and SOA Managed Server(s) ... 14-21
14.4 Configuring Other Oracle Identity Manager Installed Components ... 14-22
14.4.1 Configuring Oracle Identity Manager Server 11.1.2.2.0 ... 14-22
14.4.2 Restarting the Administration Server and SOA Managed Server ... 14-22
14.5 Upgrading Oracle Identity Manager 9.1.x.x Middle Tier ... 14-22
14.5.1 Starting and Stopping Oracle Identity Manager Managed Server(s) ... 14-23
14.5.2 Upgrading the Oracle Identity Manager Middle Tier ... 14-23
14.5.3 Restarting all the Servers ... 14-25
14.6 Post-Upgrade Steps ... 14-26
14.6.1 Optional: Configuring the Oracle Identity Manager Design Console 11.1.2.2.0 ... 14-26
14.6.2 Optional: Configuring the Oracle Identity Manager Remote Manager 11.1.2.2.0 14-26
14.6.3 Performing Post-Upgrade Tasks ... 14-26
14.6.3.1 Reviewing Performance Tuning Recommendations ... 14-27
14.6.3.2 Running the Entitlement List Schedule ... 14-27
14.6.3.3 Running the Entitlement Assignments Schedule Job ... 14-27
14.6.3.4 Running the Evaluate User Policies Scheduled Task ... 14-28
14.6.3.5 Running Catalog Synchronization ... 14-28
14.6.3.6 UMS Notification Provider ... 14-28
14.6.3.7 Upgrading User UDF ... 14-30
14.6.3.8 Upgrading Application Instances ... 14-33
14.6.3.9 Redeploying XIMDD ... 14-34
14.6.3.10 Redeploying SPML-DSML ... 14-35
14.6.3.11 Customizing Event Handlers ... 14-35
14.6.3.12 Recompiling Adapters ... 14-36
14.6.3.13 Rewriting Prepopulate Adapters ... 14-36
14.6.3.14 Disabling User Login ... 14-36
14.6.3.15 Upgrading Oracle Identity Management Reports ... 14-36
14.6.3.16 Creating New SOA Composites ... 14-36
14.6.3.17 Configuring Auto-Approval for Self-Registration ... 14-37
14.6.3.18 Generating an Audit Snapshot ... 14-37
14.6.3.19 Enabling Audit ... 14-37
14.6.3.20 Creating Password Policies ... 14-37
14.6.3.21 Reviewing OIM Data Purge Job Parameters ... 14-37
14.6.3.22 Reviewing Connector Certification ... 14-37
14.6.3.23 Verifying the Functionality of Connectors ... 14-38
14.6.4 Verifying the Upgrade ... 14-38

Part IV Upgrading Oracle Identity and Access Management High Availability Environments

15 Upgrading Oracle Access Manager High Availability Environments

15.1 Understanding Access Manager High Availability Upgrade Topology 15-1
15.2 Upgrade Roadmap..... 15-2
15.3 Shutting Down Administration Server and Managed Servers on OAMHOST1 and OAMHOST2 15-3
15.4 Backing Up the Existing Environment 15-3
15.5 Upgrading OAMHOST1 to 11.1.2.2.0 15-3
15.6 Updating Component Versions on OAMHOST1 15-4
15.7 Redeploying Access Manager Server Applications and Shared Libraries on OAMHOST1 ... 15-5
15.8 Updating Binaries of WebLogic Server and Access Manager on OAMHOST2 15-5
15.8.1 Updating Oracle WebLogic Server Binaries to 10.3.6..... 15-5
15.8.2 Updating Access Manager Binaries to 11.1.2.2.0..... 15-6
15.9 Starting Administration Server and Managed Servers on OAMHOST1 and OAMHOST2.... 15-6
15.10 Troubleshooting 15-6
15.10.1 Multi-Data Centre Feature Not Working After Upgrade 15-6

16 Upgrading Oracle Adaptive Access Manager High Availability Environments

16.1 Understanding Oracle Adaptive Access Manager High Availability Upgrade Topology..... 16-1
16.2 Upgrade Roadmap..... 16-3
16.3 Shutting Down Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2 16-3
16.4 Backing Up the Existing Environment 16-3
16.5 Updating Binaries of WebLogic Server and Oracle Adaptive Access Manager on OAAMHOST2 16-4
16.5.1 Updating Oracle WebLogic Server Binaries to 10.3.6..... 16-4
16.5.2 Updating Oracle Adaptive Access Manager Binaries to 11.1.2.2.0..... 16-4
16.6 Upgrading OAAMHOST1 to 11.1.2.2.0 16-5
16.7 Starting Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2 16-5

17 Upgrading Oracle Identity Manager High Availability Environments

17.1 Understanding Oracle Identity Manager High Availability Upgrade Topology 17-1
17.2 Upgrade Roadmap..... 17-2
17.3 Shutting Down Node Manager, Administration Server, and Managed Servers on OIMHOST1 and OIMHOST2 17-3
17.4 Backing Up the Existing Environment 17-3
17.5 Upgrading OIMHOST1 to 11.1.2.2.0 17-4
17.6 Updating Component Versions on OIMHOST1 17-4
17.7 Updating Binaries of WebLogic Server, Oracle Identity Manager, and Oracle SOA Suite on OIMHOST2 17-5
17.7.1 Updating Oracle WebLogic Server Binaries to 10.3.6..... 17-6
17.7.2 Updating Oracle SOA Suite Binaries to 11.1.1.7.0..... 17-6
17.7.3 Updating Oracle Identity Manager Binaries to 11.1.2.2.0 17-6
17.8 Replicating Domain Configuration on OIMHOST2 17-6

17.9 Upgrading Oracle Identity Manager Middle Tier on OIMHOST2 17-7
17.10 Starting Node Manager, Administration Server and Managed Servers on OIMHOST1 and OIMHOST2 17-8
17.11 Performing Post-Upgrade Tasks 17-8
17.11.1 Updating SOA Composites with OHS Attributes 17-8
17.11.2 Updating SOA Config RMI URL for Oracle Identity Manager 17-9
17.12 Troubleshooting 17-9
17.12.1 Exception in Log When Creating Users 17-9

18 Upgrading Oracle Entitlements Server High Availability Environments

18.1 Understanding Oracle Entitlements Server High Availability Upgrade Topology 18-1
18.2 Upgrade Roadmap 18-2
18.3 Shutting Down Administration Server and Managed Servers on OESHOST1 and OESHOST2 18-3
18.4 Backing Up the Existing Environment 18-3
18.5 Updating Binaries of WebLogic Server and Oracle Entitlements Server on OESHOST1 18-3
18.5.1 Updating Oracle WebLogic Server Binaries to 10.3.6 18-4
18.5.2 Updating Oracle Entitlements Server Binaries to 11.1.2.2.0 18-4
18.6 Upgrading Oracle Platform Security Services Schema on OESHOST1 18-4
18.7 Upgrading Oracle Platform Security Services on OESHOST1 18-5
18.8 Updating Binaries of WebLogic Server and Access Manager on OESHOST2 18-5
18.8.1 Updating Oracle WebLogic Server Binaries to 10.3.6 18-5
18.8.2 Updating Oracle Entitlements Server Binaries to 11.1.2.2.0 18-5
18.9 Redeploying APM Applications on OESHOST1 and OESHOST2 18-6
18.10 Starting Administration Server and Managed Servers on OESHOST1 and OESHOST2 18-7

19 Upgrading Oracle Privileged Account Manager High Availability Environments

19.1 Understanding Oracle Privileged Account Manager High Availability Upgrade Topology . 19-1
19.2 Upgrade Roadmap 19-2
19.3 Shutting Down all Servers on OPAMHOST1 and OPAMHOST2 19-3
19.4 Backing Up the Existing Environment 19-3
19.5 Updating Binaries of WebLogic Server and Oracle Privileged Account Manager on OPAMHOST1 and OPAMHOST2 19-4
19.5.1 Updating Oracle WebLogic Server Binaries to 10.3.6 on OPAMHOST1 and OPAMHOST2 19-4
19.5.2 Updating Oracle Privileged Account Manager Binaries to 11.1.2.2.0 on OPAMHOST1 and OPAMHOST2 19-4
19.6 Upgrading Database Schemas on OPAMHOST1 19-5
19.7 Starting Administration Server, Node Manager, and Managed Servers on OPAMHOST1 and OPAMHOST2 19-5
19.8 Redeploying Applications on OPAMHOST1 19-5
19.9 Verifying the Domain Upgrade 19-5
19.10 Optional: Configuring Oracle Privileged Account Manager Session Manager 19-6

19.11 Optional: Configuring Oracle Identity Navigator for WLS_OPAM1 and WLS_OPAM2 19-6

Preface

This document describes how to upgrade Oracle Identity and Access Management components to 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) documentation library:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Migration Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Release Notes*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Part I

Understanding Oracle Identity and Access Management

This part includes the following chapters:

- Chapter 1, "Introduction to Oracle Identity and Access Management Upgrade"
- Chapter 2, "Common Upgrade Tasks"

1

Introduction to Oracle Identity and Access Management Upgrade

This chapter provides an overview of Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) upgrade process and the documentation roadmap. This chapters also describes the supported upgrade scenarios for 11.1.2.2.0.

This chapter includes the following topics:

- Section 1.1, "Oracle Identity and Access Management Overview"
- Section 1.2, "Upgrade Scenarios"
- Section 1.3, "Migration and Coexistence Scenarios"
- Section 1.4, "Supported Starting Points for Upgrade on Single Node"
- Section 1.5, "Supported Starting Points for Upgrading High Availability Environments"
- Section 1.6, "Documentation Roadmap"

1.1 Oracle Identity and Access Management Overview

Oracle Identity and Access Management components enable enterprises to manage the end-to-end lifecycle of user identities across all enterprise resources - both within and beyond the firewall. With Oracle Identity and Access Management, you can deploy applications faster, apply the most granular protection to enterprise resources, automatically eliminate latent access privileges, and much more.

Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) includes the following products:

- Oracle Access Management, which includes the following components:
  - Oracle Access Management Access Manager
  - Oracle Access Management Identity Federation
  - Oracle Access Management Mobile and Social
  - Oracle Access Management Security Token Service
- Oracle Adaptive Access Manager
- Oracle Identity Manager
- Oracle Entitlements Server
- Oracle Privileged Account Manager

- Oracle Identity Navigator

1.2 Upgrade Scenarios

The term **Upgrade** refers to the upgrade of existing Oracle Identity and Access Management 11*g* Release 1 and 11*g* Release 2 components to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server. For each of these upgrade scenarios, you use the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) installer to update your existing Oracle Home (*IAM_HOME*) to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0).

You can upgrade the following Oracle Identity and Access Management components to Oracle Identity and Access Management 11.1.2.2.0:

- Oracle Identity and Access Management 11*g* Release 2 (11.1.2.1.0) Components
  - Oracle Access Manager 11.1.2.1.0
  - Oracle Adaptive Access Manager 11.1.2.1.0
  - Oracle Identity Manager 11.1.2.1.0
  - Oracle Entitlements Server 11.1.2.1.0
  - Oracle Privileged Account Manager 11.1.2.1.0
  - Oracle Identity Navigator 11.1.2.1.0
- Oracle Identity and Access Management 11*g* Release 2 (11.1.2) Components
  - Oracle Access Manager 11.1.2
  - Oracle Adaptive Access Manager 11.1.2
  - Oracle Identity Manager 11.1.2
  - Oracle Entitlements Server 11.1.2
  - Oracle Privileged Account Manager 11.1.2
  - Oracle Identity Navigator 11.1.2
- Oracle Identity and Access Management 11*g* Release 1 (11.1.1.7.0) Components
  - Oracle Access Manager 11.1.1.7.0
  - Oracle Adaptive Access Manager 11.1.1.7.0
  - Oracle Identity Manager 11.1.1.7.0
  - Oracle Identity Navigator 11.1.1.7.0
- Oracle Identity and Access Management 11*g* Release 1 (11.1.1.5.0) Components
  - Oracle Access Manager 11.1.1.5.0
  - Oracle Adaptive Access Manager 11.1.1.5.0
  - Oracle Identity Manager 11.1.1.5.0
  - Oracle Entitlements Server 11.1.1.5.0
  - Oracle Identity Navigator 11.1.1.5.0
- Oracle Identity Manager 9.1.x.x

Note: This guide covers the procedures for all the upgrade scenarios described in this section.

1.3 Migration and Coexistence Scenarios

The term **Migration** refers to the migration of 10*g* version of Oracle Identity and Access Management components or Sun products to Oracle Identity and Access Management 11.1.2.2.0, scenarios where you migrate the following products to Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0). In these migration scenarios, you must install a new 11*g* Release 2 (11.1.2.2.0) Oracle Home (`IAM_HOME`) and then migrate your configuration data from your previous installation to the new 11*g* Release 2 (11.1.2.2.0) Oracle Home.

- Oracle Access Manager 10*g*
- Oracle Adaptive Access Manager 10*g*
- Oracle Single Sign-On 10*g*
- Sun OpenSSO Enterprise 8.0
- Sun Java System Access Manager 7.1
- Oracle Identity Analytics

During migration, you can have both the old and the new deployments coexisting, such that some applications are protected by the old server, and the others are protected by the new server. The coexistence mode allows you to have seamless single sign-on experience when you navigate between applications protected by different servers.

For example, Sun OpenSSO Enterprise 8.0 and Oracle Access Management Access Manager 11.1.2.2.0 servers can coexist and work together, so that the you have seamless single sign-on experience when you navigate between applications protected by Sun OpenSSO Enterprise 8.0 and Oracle Access Management Access Manager 11.1.2.2.0 Servers.

The following are the coexistence scenarios supported in 11*g* Release 2 (11.1.2.2.0):

- Coexistence of Oracle Access Manager 10*g* with Oracle Access Management Access Manager 11.1.2.2.0
- Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2.2.0
- Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2.2.0

Note: This guide covers only the upgrade scenarios described in Section 1.2, "Upgrade Scenarios".

The migration and coexistence scenarios are covered in the *Oracle Fusion Middleware Migration Guide for Oracle Identity and Access Management*.

1.4 Supported Starting Points for Upgrade on Single Node

This section describes the supported starting points for Oracle Identity and Access Management upgrade on a single node.

This section contains the following sub-sections:

- Supported Starting Points for Oracle Access Manager Upgrade
- Supported Starting Points for Oracle Adaptive Access Manager Upgrade
- Supported Starting Points for Oracle Identity Manager Upgrade
- Supported Starting Points for Oracle Entitlements Server Upgrade
- Supported Starting Points for Oracle Privileged Account Manager Upgrade
- Supported Starting Points for Oracle Identity Navigator Upgrade

1.4.1 Supported Starting Points for Oracle Access Manager Upgrade

Table 1–1 lists the supported starting points for upgrading Oracle Access Manager to 11*g* Release 2 (11.1.2.2.0) on a single node:

Table 1–1 Oracle Access Manager Releases Supported for Upgrade

Release	Supported Bundle Patch
11*g* Release 2 (11.1.2.1.0)	▪ Bundle Patch 11.1.2.1.1
11*g* Release 2 (11.1.2)	▪ Bundle Patch 11.1.2.0.3 ▪ Bundle Patch 11.1.2.0.2 ▪ Bundle Patch 11.1.2.0.1
11*g* Release 1 (11.1.1.7.0)	▪ Bundle Patch 11.1.1.7.0 OAM-FAREL8-BP ▪ Bundle Patch 11.1.1.7.0 OAM-FAREL7-BP
11*g* Release 1 (11.1.1.5.0)	▪ Bundle Patch 11.1.1.5.5 ▪ Bundle Patch 11.1.1.5.4 ▪ Bundle Patch 11.1.1.5.3 ▪ Bundle Patch 11.1.1.5.2 ▪ Bundle Patch 11.1.1.5.1
10*g* (10.1.4.3)	This version is supported for migration.

Note: Moving from Oracle Access Manager 10*g* to Oracle Access Management Access Manager 11.1.2.2.0 is referred to as migration, and the procedure is documented in the Oracle Fusion Middleware Migration Guide for Oracle Identity and Access Management.

1.4.2 Supported Starting Points for Oracle Adaptive Access Manager Upgrade

Table 1–2 lists the supported starting points for upgrading Oracle Adaptive Access Manager to 11*g* Release 2 (11.1.2.2.0) on a single node:

Table 1–2 Oracle Adaptive Access Manager Releases Supported for Upgrade

Release	Supported Bundle Patch
11*g* Release 2 (11.1.2.1.0)	▪ All Bundle Patches are supported

Table 1–2 (Cont.) Oracle Adaptive Access Manager Releases Supported for Upgrade

Release	Supported Bundle Patch
11*g* Release 2 (11.1.2)	■ All Bundle Patches are supported
11*g* Release 1 (11.1.1.7.0)	■ All Bundle Patches are supported
11*g* Release 1 (11.1.1.5.0)	■ Bundle Patch 11.1.1.5.1 ■ Bundle Patch 11.1.1.5.2
10*g* (10.1.4.5)	■ Bundle Patch 15

Note: Moving from Oracle Adaptive Access Manager 10*g* (10.1.4.5) to Oracle Adaptive Access Manager 11.1.2.2.0 is referred to as migration, and the procedure is documented in the Migration Guide for Oracle Identity and Access Management.

1.4.3 Supported Starting Points for Oracle Identity Manager Upgrade

Table 1–3 lists the supported starting points for upgrading Oracle Identity Manager to 11*g* Release 2 (11.1.2.2.0) on a single node:

Table 1–3 Oracle Identity Manager Releases Supported for Upgrade

Release	Supported Bundle Patch
11*g* Release 2 (11.1.2.1.0)	■ All Bundle Patches are supported
11*g* Release 2 (11.1.2)	■ All Bundle Patches are supported
11*g* Release 1 (11.1.1.7.0)	■ All Bundle Patches are supported
11*g* Release 1 (11.1.1.5.0)	■ All Bundle Patches are supported
9.1.x.x	■ Bundle Patches 9.1.0.1 and higher

1.4.4 Supported Starting Points for Oracle Entitlements Server Upgrade

Table 1–4 lists the supported starting points for upgrading Oracle Entitlements Server to 11*g* Release 2 (11.1.2.2.0) on a single node:

Table 1–4 Oracle Entitlements Server Releases Supported for Upgrade

Release	Supported Bundle Patch
11*g* Release 2 (11.1.2.1.0)	■ All Bundle Patches are supported
11*g* Release 2 (11.1.2)	■ All Bundle Patches are supported
11*g* Release 1 (11.1.1.5.0)	■ Bundle Patch 11.1.1.5.1

1.4.5 Supported Starting Points for Oracle Privileged Account Manager Upgrade

Table 1–5 lists the supported starting points for upgrading Oracle Privileged Account Manager to 11*g* Release 2 (11.1.2.2.0):

Table 1–5 Oracle Privileged Account Manager Releases Supported for Upgrade

Release	Supported Bundle Patch
11*g* Release 2 (11.1.2.1.0)	■ All Bundle Patches are supported
11*g* Release 2 (11.1.2)	■ All Bundle Patches are supported

1.4.6 Supported Starting Points for Oracle Identity Navigator Upgrade

Table 1–6 lists the supported starting points for upgrading Oracle Entitlements Server to 11*g* Release 2 (11.1.2.2.0) on a single node:

Table 1–6 Oracle Identity Navigator Releases Supported for Upgrade

Release	Supported Bundle Patch
11*g* Release 2 (11.1.2.1.0)	■ All Bundle Patches are supported
11*g* Release 2 (11.1.2)	■ All Bundle Patches are supported
11*g* Release 1 (11.1.1.7.0)	■ All Bundle Patches are supported
11*g* Release 1 (11.1.1.5.0)	■ All Bundle Patches are supported

1.5 Supported Starting Points for Upgrading High Availability Environments

Table 1–7 lists the supported starting points for upgrading high availability environments of various components of Oracle Identity and Access Management to 11*g* Release 2 (11.1.2.2.0):

Table 1–7 Oracle Identity and Access Management Releases Supported for High Availability Upgrade

Component	Supported Starting Point
Oracle Access Manager	■ 11*g* Release 2 (11.1.2.1.0) ■ 11*g* Release 1 (11.1.1.5.0)
Oracle Adaptive Access Manager	■ 11g Release 2 (11.1.2.1.0) ■ 11g Release 1 (11.1.1.5.0)
Oracle Identity Manager	■ 11*g* Release 2 (11.1.2.1.0) ■ 11*g* Release 2 (11.1.2) ■ 11*g* Release 1 (11.1.1.5.0)
Oracle Entitlements Server	■ 11g Release 2 (11.1.2.1.0)
Oracle Privileged Account Manager	■ 11g Release 2 (11.1.2.1.0)

1.6 Documentation Roadmap

This section provides the documentation roadmap for all the upgrade scenarios on Oracle WebLogic Server.

> **Note:** For information about upgrading Oracle Identity and Access Management components on IBM WebSphere, see *Oracle Fusion Middleware Third-Party Application Server Guide for Oracle Identity and Access Management*.

Table 1–8 lists all the upgrade scenarios, and the chapters in which the respective upgrade procedure is described. Depending on the upgrade scenario, go to the respective chapter, and follow the procedure.

Table 1–8 Documentation Roadmap for Oracle Identity and Access Management Upgrade

Upgrade Scenarios	Chapter
Oracle Identity and Access Management 11.1.2.1.0 and 11.1.2 Upgrade on a Single Node	
Oracle Access Management Access Manager 11.1.2.1.0 to Oracle Access Management Access Manager 11.1.2.2.0 Upgrade	Chapter 3, "Upgrading Oracle Access Manager 11g Release 2 (11.1.2.x.x) Environments"
Oracle Access Management Access Manager 11.1.2 to Oracle Access Management Access Manager 11.1.2.2.0 Upgrade	
Oracle Adaptive Access Manager 11.1.2.1.0 to Oracle Adaptive Access Manager 11.1.2.2.0 Upgrade	Chapter 4, "Upgrading Oracle Adaptive Access Manager 11g Release 2 (11.1.2.x.x) Environments"
Oracle Adaptive Access Manager 11.1.2 to Oracle Adaptive Access Manager 11.1.2.2.0 Upgrade	
Oracle Identity Manager 11.1.2.1.0 to Oracle Identity Manager 11.1.2.2.0 Upgrade	Chapter 5, "Upgrading Oracle Identity Manager 11g Release 2 (11.1.2.x.x) Environments"
Oracle Identity Manager 11.1.2 to Oracle Identity Manager 11.1.2.2.0 Upgrade	
Oracle Entitlements Server 11.1.2.1.0 to Oracle Entitlements Server 11.1.2.2.0 Upgrade	Chapter 6, "Upgrading Oracle Entitlements Server 11g Release 2 (11.1.2.x.x) Environments"
Oracle Entitlements Server 11.1.2 to Oracle Entitlements Server 11.1.2.2.0 Upgrade	

Table 1–8 (Cont.) Documentation Roadmap for Oracle Identity and Access Management Upgrade

Upgrade Scenarios	Chapter
Oracle Privileged Account Manager 11.1.2.1.0 to Oracle Privileged Account Manager 11.1.2.2.0 Upgrade	Chapter 7, "Upgrading Oracle Privileged Account Manager 11g Release 2 (11.1.2.x.x) Environments"
Oracle Privileged Account Manager 11.1.2 to Oracle Privileged Account Manager 11.1.2.2.0 Upgrade	
Oracle Identity Navigator 11.1.2.1.0 to Oracle Identity Navigator 11.1.2.2.0 Upgrade	Chapter 8, "Upgrading Oracle Identity Navigator 11g Release 2 (11.1.2.x.x) Environments"
Oracle Identity Navigator 11.1.2.1.0 to Oracle Identity Navigator 11.1.2.2.0 Upgrade	
Oracle Identity and Access Management 11.1.1.7.0, 11.1.1.5.0, and 9.1.x.x Upgrade on a Single Node	
Oracle Access Manager 11.1.1.7.0 to Oracle Access Management Access Manager 11.1.2.2.0 Upgrade	Chapter 9, "Upgrading Oracle Access Manager 11g Release 1 (11.1.1.x.x) Environments"
Oracle Access Manager 11.1.1.5.0 to Oracle Access Management Access Manager 11.1.2.2.0 Upgrade	
Oracle Adaptive Access Manager 11.1.1.7.0 to Oracle Adaptive Access Manager 11.1.2.2.0 Upgrade	Chapter 10, "Upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x) Environments"
Oracle Adaptive Access Manager 11.1.1.5.0 to Oracle Adaptive Access Manager 11.1.2.2.0 Upgrade	
Oracle Identity Manager 11.1.1.7.0 to Oracle Identity Manager 11.1.2.2.0 Upgrade	Chapter 11, "Upgrading Oracle Identity Manager 11g Release 1 (11.1.1.x.x) Environments"
Oracle Identity Manager 11.1.1.5.0 to Oracle Identity Manager 11.1.2.2.0 Upgrade	
Oracle Identity Manager 9.1.x.x to Oracle Identity Manager 11.1.2.2.0 Upgrade	Chapter 14, "Upgrading Oracle Identity Manager 9.1.x.x Environments"
Oracle Entitlements Server 11.1.1.5.0 to Oracle Entitlements Server 11.1.2.2.0 Upgrade	Chapter 12, "Upgrading Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) Environment"

Table 1–8 (Cont.) Documentation Roadmap for Oracle Identity and Access Management Upgrade

Upgrade Scenarios	Chapter
Oracle Identity Navigator 11.1.1.7.0 to Oracle Identity Navigator 11.1.2.2.0 Upgrade	Chapter 13, "Upgrading Oracle Identity Navigator 11g Release 1 (11.1.1.x.x) Environments"
Oracle Identity Navigator 11.1.1.5.0 to Oracle Identity Navigator 11.1.2.2.0 Upgrade	
Oracle Identity and Access Management High Availability Upgrade	
Oracle Access Manager High Availability Upgrade	Chapter 15, "Upgrading Oracle Access Manager High Availability Environments"
Oracle Adaptive Access Manager High Availability Upgrade	Chapter 16, "Upgrading Oracle Adaptive Access Manager High Availability Environments"
Oracle Identity Navigator High Availability Upgrade	Chapter 17, "Upgrading Oracle Identity Manager High Availability Environments"
Oracle Entitlements Server High Availability Upgrade	Chapter 18, "Upgrading Oracle Entitlements Server High Availability Environments"
Oracle Privileged Account Manager High Availability Upgrade	Chapter 19, "Upgrading Oracle Privileged Account Manager High Availability Environments"

2

Common Upgrade Tasks

This chapter lists the upgrade tasks that need to be performed as part of the upgrade process.

> **Note:** This chapter contains the upgrade tasks that are common to different upgrade scenarios. You do not have to perform all the tasks described in this chapter. Refer to the Section 1.6, "Documentation Roadmap" for the upgrade roadmap.

This chapter includes the following topics:

- Section 2.1, "Reviewing System Requirements and Certification"
- Section 2.2, "Backing up the Existing Environment"
- Section 2.3, "Upgrading to Oracle WebLogic Server 10.3.6"
- Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)"
- Section 2.5, "Creating Database Schemas Using Repository Creation Utility"
- Section 2.6, "Upgrading Schemas Using Patch Set Assistant"
- Section 2.7, "Upgrading Oracle Platform Security Services"
- Section 2.8, "Stopping the Servers"
- Section 2.9, "Starting the Servers"

2.1 Reviewing System Requirements and Certification

Before performing any installation, upgrade, or migration, you should read the system requirements and certification documents to ensure that your environment meets the minimum requirements for the products you are installing or upgrading to.

- *Oracle Fusion Middleware System Requirements and Specifications*

  This document contains information related to hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches.

- *Oracle Fusion Middleware Supported System Configurations*

  This document contains information related to supported installation types, platforms, operating systems, databases, JDKs, and third-party products.

- For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

  This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

2.2 Backing up the Existing Environment

To back up the existing environment, you must stop all the servers, and back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Database schemas

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

2.3 Upgrading to Oracle WebLogic Server 10.3.6

To upgrade Oracle WebLogic Server to 10.3.6, complete the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

   For more information, see "Downloading an Upgrade Installer From My Oracle Support" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

   For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2.4 Updating Oracle Identity and Access Management Binaries to 11*g* Release 2 (11.1.2.2.0)

To update the existing Oracle Identity and Access Management binaries to 11.1.2.2.0, you must use the Oracle Identity and Access Management 11.1.2.2.0 installer. To do this, perform the following tasks:

- Obtaining the Software
- Starting the Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) Installer
- Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)

2.4.1 Obtaining the Software

For more information on obtaining Oracle Fusion Middleware 11*g* software, see *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.

2.4.2 Starting the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Installer

This topic explains how to start the Oracle Identity and Access Management Installer.

Notes:

- If you are installing on an IBM AIX operating system, you must run the `rootpre.sh` script from the `Disk1` directory before you start the Installer.
- Starting the Installer as the `root` user is not supported.

Start the Installer by doing the following:

On UNIX:

1. Move from your present working directory to the directory where you extracted the contents of the Installer to.
2. Move to the following location:

   ```
   cd Disk1
   ```

3. Run the following command:

   ```
   ./runInstaller -jreLoc <full path to the JRE directory>
   ```

   For example:

   ```
   ./runInstaller -jreLoc <MW_HOME>/jdk160_29/jre
   ```

On Windows:

1. Move from your present working directory to the directory where you extracted the contents of the Installer to.
2. Move to the following location:

   ```
   cd Disk1
   ```

3. Run the following command:

   ```
   setup.exe -jreLoc <full path to the JRE directory>
   ```

   For Example:

   ```
   setup.exe -jreLoc <MW_HOME>\jdk160_29\jre
   ```

Note: If you do not specify the `-jreLoc` option on the command line when using the Oracle JRockit JDK, the following warning message is displayed:

```
-XX:MaxPermSize=512m is not a valid VM option. Ignoring
```

This warning message does not affect the installation. You can continue with the installation.

On 64-bit platforms, when you install Oracle WebLogic Server using the generic jar file, the `jrockit_1.6.0_29` directory is not created in your Middleware Home. You must enter the absolute path to the JRE folder from where your JDK is located.

2.4.3 Installing Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0)

Use the Oracle Identity and Access Management 11.1.2.2.0 Installer to upgrade existing Oracle Identity and Access Management binaries to 11.1.2.2.0:

1. After you start the Installer, the **Welcome** screen appears.
2. Click **Next** on the **Welcome** screen. The **Install Software Updates** screen appears. Select whether or not you want to search for updates. Click **Next**.
3. The **Prerequisite Checks** screen appears. If all prerequisite checks pass inspection, click **Next**. The **Specify Installation Location** screen appears.
4. On the **Specify Installation Location** screen, point to the Middleware Home to your existing Middleware Home installed on your system.
5. In the **Oracle Home Directory** field, specify the path of the existing Oracle Identity and Access Management Home. This directory is also referred to as `<IAM_HOME>` in this book.

   Click **Next**. The **Installation Summary** screen appears.
6. The **Installation Summary** screen displays a summary of the choices that you made. Review this summary and decide whether you want to proceed with the installation. If you want to modify any of the configuration settings at this stage, select a topic in the left navigation page and modify your choices. To continue installing Oracle Identity and Access Management, click **Install**. The **Installation Progress** screen appears.
7. Monitor the progress of your installation. The location of the installation log file is listed for reference. After the installation progress reaches 100%, click **OK**. If you encounter any issue, check the log file. For information about locating the log files, see "Locating Installation Log Files" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

   Note: If you cancel or abort when the installation is in progress, you must manually delete the `<IAM_HOME>` directory before you can reinstall the Oracle Identity and Access Management software.

   To invoke online help at any stage of the installation process, click **Help** on the installation wizard screens.

   ---

8. The **Installation Complete** screen appears. On the **Installation Complete** screen, click **Finish**.

   This installation process copies the 11.1.2.2.0 Oracle Identity and Access Management software to your system.

For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2.2.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

2.5 Creating Database Schemas Using Repository Creation Utility

To create 11.1.2.2.0 Database schemas, you must use Repository Creation Utility (RCU). When you create new schemas, do not delete your existing schemas, and do not use the old schema name, as you will need the old schema credentials while exporting the Access Data.

To create the database schemas, perform the following tasks:

1. Obtaining Repository Creation Utility
2. Starting Repository Creation Utility
3. Creating Schemas

2.5.1 Obtaining Repository Creation Utility

Download the Repository Creation Utility. For information about obtaining Repository Creation Utility, see "Obtaining RCU" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

2.5.2 Starting Repository Creation Utility

Start the Repository Creation Utility from the location where you downloaded it. For information about starting Repository Creation Utility, see "Starting RCU" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

2.5.3 Creating Schemas

Create the necessary schemas using Repository Creation Utility. For information about creating schemas, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

2.6 Upgrading Schemas Using Patch Set Assistant

To upgrade the existing schemas to 11.1.2.2.0, you must use the Patch Set Assistant. To upgrade the database schemas, perform the following tasks:

- Checking Your Database and Schemas
- Starting Patch Set Assistant
- Using the Patch Set Assistant Graphical Interface to Upgrade Schemas
- Verifying Schema Upgrade

2.6.1 Checking Your Database and Schemas

Before running Patch Set Assistant, you should make sure that your database is running and that the schemas are supported for upgrade. To check this, run the following SQL command:

```
SELECT OWNER, VERSION, STATUS, UPGRADED FROM SCHEMA_VERSION_REGISTRY;
```

Table 2–1 lists the schemas and their versions supported for upgrade:

Table 2–1 Schemas and Their Versions Supported for Upgrade

Schema Name	Schema Version(s) Supported for Upgrade
Oracle Access Manager (OAM)	11.1.1.3.0 11.1.2.1.0
Oracle Adaptive Access Manager (OAAM)	11.1.1.3.0 11.1.2.0.0

Table 2–1 (Cont.) Schemas and Their Versions Supported for Upgrade

Schema Name	Schema Version(s) Supported for Upgrade
Oracle Identity Manager (OIM)	11.1.1.3.0
	11.1.1.5.0
	11.1.1.7.0
	11.1.2.0.0
	11.1.2.1.0
Oracle Privileged Account Manager (OPAM)	11.1.2.0.0
	11.1.2.1.0
Oracle Platform Security Services (OPSS)	11.1.1.6.0

2.6.2 Starting Patch Set Assistant

To start Patch Set Assistant, do the following:

On UNIX:

1. Move from your present working directory to the `<MW_HOME>/oracle_common/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/oracle_common/bin
   ```

2. Run the following command:

   ```
   ./psa
   ```

On Windows:

1. Move from your present working directory to the `<MW_HOME>\oracle_common\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\oracle_common\bin
   ```

2. Execute the following command:

   ```
   psa.bat
   ```

2.6.3 Using the Patch Set Assistant Graphical Interface to Upgrade Schemas

After starting the Patch Set Assistant Installer, follow the instructions on the screen to update your schemas.

Follow the instructions in Table 2–2 to update your schemas:

Table 2–2 Patch Set Assistant Screens

Screen	Description
Welcome	This page introduces you to the Patch Set Assistant.
Select Component	Select the component you wish to upgrade.
Prerequisite	Verify that you have satisfied the database prerequisites.

Table 2–2 (Cont.) Patch Set Assistant Screens

Screen	Description
Schema	Specify your database credentials to connect to your database, then select the schema you want to update. Note that this screen appears once for each schema that must be updated as a result of the component you selected on the Select Component screen.
Examine	This page displays the status of the Patch Set Assistant as it examines each component schema. Verify that your schemas have a "successful" indicator in the Status column.
Upgrade Summary	Verify that the schemas are the ones you want to upgrade.
Upgrade Progress	This screen shows the progress of the schema upgrade.
Upgrade Success	Once the upgrade is successful, you get this screen.

2.6.4 Verifying Schema Upgrade

You can verify the schema upgrade by checking out the log files. The Patch Set Assistant writes log files in the following locations:

On UNIX:

`<MW_HOME>/oracle_common/upgrade/logs/psa/psatimestamp.log`

On Windows:

`<MW_HOME>\oracle_common\upgrade\logs\psa\psatimestamp.log`

Some components create a second log file named `psatimestamp.out` in the same location.

The `timestamp` reflects the actual date and time when Patch Set Assistant was run.

If any failures occur when running Patch Set Assistant, you can use these log files to help diagnose and correct the problem. Do not delete them. You can alter the contents of the log files by specifying a different `-logLevel` from the command line.

Some of the operations performed by Patch Set Assistant may take longer to complete than others. If you want to see the progress of these long operations, you can see this information in the log file, or you can use the following query:

```
SELECT VERSION, STATUS, UPGRADED FROM SCHEMA_VERSION_REGISTRY WHERE
OWNER='schema_name';
```

In the query results, the `STATUS` field is either `UPGRADING` or `UPGRADED` during the schema patching operation, and becomes `VALID` when the operation is completed.

2.7 Upgrading Oracle Platform Security Services

This section describes how to upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores to 11.1.2.2.0. It upgrades the `jps-config.xml` file and policy stores.

To upgrade Oracle Platform Security Services for LDAP- or DB-based store, complete the following steps:

1. Run the following command from the location *`MW_HOME`*`/oracle_common/common/bin` to launch the WebLogic Scripting Tool (WLST):

   On UNIX:

```
./wlst.sh
```

On Windows:

```
wlst.cmd
```

2. Run the following command to upgrade OPSS:

```
upgradeOpss(jpsConfig="<absolute_path_to_old_version_jps-config.xml_file>",
            jaznData="<absolute_path_to_new_version_OOTB_JAZN_data_file>",
            auditStore="<absolute_path_to_OOTB_audit-store.xml_file>",
            jdbcDriver="<jdbc_driver>",
            url="<jdbc_ldap_url>",
            user="<jdbc_ldap_user>",
            password="<jdbc_ldap_password>"],
            upgradeJseStoreType="true/false"])
```

Table 2–3 describes the arguments of the `upgradeOpss` command:

Table 2–3 Arguments to be Specified While Running upgradeOpss command

Argument	When to Use?	Mandatory/Optional	Description
`jpsConfig`	Use this argument if you are upgrading Oracle Identity and Access Management 11*g* Release 1 (11.1.1.x.x) or 11*g* Release 2 (11.1.2.x.x) to 11*g* Release 2 (11.1.2.2.0).	This argument is mandatory for both DB-based and LDAP-based store.	Specify the absolute path to the location of 11.1.2.x.x `jps-config.xml` domain configuration file. The `upgradeOpss` script backs up the `jps-config.xml` file in the same directory as a file with the suffix `.bak` appended to the its name. The `jps-config.xml` file is typically located in the directory *`$DOMAIN_HOME`*`/config/fmwconfig`. The file `jps-config-jse.xml` is assumed to be located in the same directory.
`jaznData`	Use this argument if you are upgrading Oracle Identity and Access Management 11*g* Release 1 (11.1.1.x.x) or 11*g* Release 2 (11.1.2.x.x) to 11*g* Release 2 (11.1.2.2.0).	This argument is mandatory for both DB-based and LDAP-based store.	Specify the absolute path to the location of 11.1.2.x.x out-of-the-box `system-jazn-data.xml` file. The system-jazn-data.xml file is typically located in the directory `$oracle_common/modules/oracle.jps_11.1.1/domain_config`.
`auditStore`	Use this argument if you are upgrading Oracle Identity and Access Management 11*g* Release 2 (11.1.2.x.x) to 11*g* Release 2 (11.1.2.2.0).	This argument is optional for both DB-based and LDAP-based store.	Specify the absolute path to the location of 11.1.2.x.x out-of-the-box `audit-store.xml` file. If unspecified, it defaults to the file `audit_store.xml` located in the directory specified for the argument `jaznData`.

Table 2–3 (Cont.) Arguments to be Specified While Running upgradeOpss command

Argument	When to Use?	Mandatory/Optional	Description
`jdbcDriver`	Use this argument if you are upgrading Oracle Identity and Access Management 11*g* Release 2 (11.1.2.x.x) to 11*g* Release 2 (11.1.2.2.0).	This argument is required only in case of DB-based store.	Specify the JDBC driver to the store.
`url`	Use this argument if you are upgrading Oracle Identity and Access Management 11*g* Release 2 (11.1.2.x.x) to 11*g* Release 2 (11.1.2.2.0).	This argument is mandatory for both DB-based and LDAP-based store.	Specify the JDBC URL or LDAP URL in the format: *driverType*:*host*:*port*/*service name* If unspecified, the JDBC URL or LDAP URL is read from the configuration file.
`user`	Use this argument if you are upgrading Oracle Identity and Access Management 11*g* Release 2 (11.1.2.x.x) to 11*g* Release 2 (11.1.2.2.0).	This argument is mandatory in case of DB-based store, whereas it is optional for LDAP-based store.	Specify the JDBC user name or LDAP bind name. If not specified, the value is read from the configuration file. In case of LDAP-based store, the user performing the upgrade must have read and write privileges to the schema, the root node, and all nodes under `cn=OPSS,cn=OracleSchemaVersion`. In case of a DB-based store, perform the upgrade as the OPSS DB schema user.
`password`	Use this argument if you are upgrading Oracle Identity and Access Management 11*g* Release 2 (11.1.2.x.x) to 11*g* Release 2 (11.1.2.2.0).	This argument is mandatory in case of DB-based store, whereas it is optional for LDAP-based store.	Specify the JDBC password in case of DB-based store, or the LDAP bind password in case of LDAP-based store. If not specified, it is read from the configuration file.

Table 2–3 (Cont.) Arguments to be Specified While Running upgradeOpss command

Argument	When to Use?	Mandatory/Optional	Description
`upgradeJseStoreType`	Use this argument if you are upgrading Oracle Identity and Access Management 11*g* Release 2 (11.1.2.x.x) to 11*g* Release 2 (11.1.2.2.0).	This argument is optional for both LDAP-based and DB-based store.	This argument indicates whether the store type configuration (in the file `jps-config-jse.xml`) should be changed from file-based to LDAP-based or DB-based; the type selected being same to the store type specified in the file `jps-config.xml`. Set the value of this argument to `true` if you wish to modify the store type configuration; or set it to `false` to keep the file-based configuration. The default value is `false`.

For example:

On UNIX:

```
upgradeOpss(jpsConfig="/Oracle/Middleware/user_projects/domains/oes_
domain/config/fmwconfig/jps-config.xml",
jaznData="/oracle/middleware/oracle_common/modules/oracle.jps_11.1.1/domain_
config/system-jazn-data.xml",
jdbcDriver="oracle.jdbc.OracleDriver",
url="jdbc:oracle:thin:@host:1234/db123",
user="R2_OPSS",
password="password123",
upgradeJseStoreType="true")
```

On Windows:

```
upgradeOpss(jpsConfig="C:\\Oracle\\Middleware\\user_projects\\domains\\oes_
domain\\config\\fmwconfig\\jps-config.xml",
jaznData="C:\\oracle\\middleware\\oracle_common\\modules\\oracle.jps_
11.1.1\\domain_config\\system-jazn-data.xml",
jdbcDriver="oracle.jdbc.OracleDriver",
url="jdbc:oracle:thin:@host:1234/db123",
user="R2_OPSS",
password="password123",
upgradeJseStoreType="true")
```

2.8 Stopping the Servers

To stop the WebLogic Administration Server and the Managed Server(s), refer to the following sections:

- Stopping the Managed Server(s)
- Stopping the WebLogic Administration Server
- Stopping the Node Manager

You must stop the Managed Server(s) first, and then the WebLogic Administration Server.

2.8.1 Stopping the Managed Server(s)

To stop the Managed Server(s), do the following:

On UNIX:

1. Move from your present working directory to the *MW_HOME*/user_projects/domains/*domain_name*/bin directory by running the following command on the command line:

   cd *MW_HOME*/user_projects/domains/*domain_name*/bin

2. Run the following command to stop the servers:

   ./stopManagedWebLogic.sh *managed_server_name admin_url admin_username password*

   where

   managed_server_name is the name of the Managed Server.

   admin_url is URL of the WebLogic administration console. Specify it in the format http://*host*:*port*/console. Specify only if the WebLogic Administration Server is on a different computer.

   admin_username is the username of the WebLogic Administration Server.

   password is the password of the WebLogic Administration Server.

For example:

```
./stopManagedWebLogic.sh oim_server1 http://host.example.com:7001/console
weblogic password123
```

On Windows:

1. Move from your present working directory to the *MW_HOME*\user_projects\domains*domain_name*\bin directory by running the following command on the command line:

   cd *MW_HOME*\user_projects\domains*domain_name*\bin

2. Run the following command to stop the Managed Servers:

   stopManagedWebLogic.cmd *managed_server_name admin_url admin_username password*

   where

   managed_server_name is the name of the Managed Server.

   admin_url is URL of the WebLogic administration console. Specify it in the format http://*host*:*port*/console. specify only if the WebLogic Administration Server is on a different computer.

   admin_username is the username of the WebLogic Administration Server.

   password is the password of the WebLogic Administration Server.

For example:

```
stopManagedWebLogic.cmd oim_server1 http://host.example.com:7001/console
weblogic password123
```

For more information, see "Stopping the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

2.8.2 Stopping the WebLogic Administration Server

To stop the WebLogic Administration Server, do the following:

On UNIX:

Run the following commands:

```
cd MW_HOME/user_projects/domains/domain_name/bin
./stopWebLogic.sh
```

On Windows:

Run the following commands:

```
cd MW_HOME\user_projects\domains\domain_name\bin
stopWebLogic.cmd
```

2.8.3 Stopping the Node Manager

To stop the Node Manager, close the command shell in which it is running.

Alternatively, after having set the attribute `QuitEnabled` to `true` (the default is `false`) in `nodemanager.properties` file, you can use WLST command to connect to the Node Manager and shut it down. For more information, see "stopNodeManager" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

2.9 Starting the Servers

To start the WebLogic Administration Server and the Managed Server(s), refer to the following sections:

- Starting the Node Manager
- Starting the WebLogic Administration Server
- Starting the Managed Server(s)

2.9.1 Starting the Node Manager

To start the Node Manager, you must run the command `startNodeManager.sh` (on UNIX) or `startNodeManager.cmd` (on Windows) from the location *$WL_HOME*`/server/bin`.

For more information, see "startNodeManager" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

2.9.2 Starting the WebLogic Administration Server

To start the WebLogic Administration Server, do the following:

On UNIX:

Run the following commands:

```
cd MW_HOME/user_projects/domains/domain_name/bin
./startWebLogic.sh
```

On Windows:

Run the following commands:

```
cd MW_HOME\user_projects\domains\domain_name\bin

startWebLogic.cmd
```

2.9.3 Starting the Managed Server(s)

To start the Managed Server(s), do the following:

On UNIX:

1. Move from your present working directory to the *MW_HOME*/user_projects/domains/*domain_name*/bin directory by running the following command on the command line:

   ```
   cd MW_HOME/user_projects/domains/domain_name/bin
   ```

2. Run the following command to start the Managed Servers:

   ```
   ./startManagedWebLogic.sh managed_server_name admin_url admin_username password
   ```

   where

   managed_server_name is the name of the Managed Server

   admin_url is URL of the administration console. Specify it in the format http://*host*:*port*/console. Specify only if the WebLogic Administration Server is on a different computer.

   admin_username is the username of the WebLogic Administration Server.

   password is the password of the WebLogic Administration Server.

For example:

```
./startManagedWebLogic.sh oim_server1 http://host.example.com:7001/console
weblogic password123
```

On Windows:

1. Move from your present working directory to the *MW_HOME*\user_projects\domains*domain_name*\bin directory by running the following command on the command line:

   ```
   cd MW_HOME\user_projects\domains\domain_name\bin
   ```

2. Run the following command to start the Managed Servers:

   ```
   startManagedWebLogic.cmd managed_server_name admin_url admin_username password
   ```

   where

   managed_server_name is the name of the Managed Server.

   admin_url is URL of the administration console. Specify it in the format http://*host*:*port*/console. Specify only if the WebLogic Administration Server is on a different computer.

   admin_username is the username of the WebLogic Administration Server.

   password is the password of the WebLogic Administration Server.

For example:

```
startManagedWebLogic.cmd oim_server1 http://host.example.com:7001/console
weblogic password123
```

For more information, see "Starting the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Part II

Upgrading Oracle Identity and Access Management 11*g* Release 2 (11.1.2.x.x) Environments

This part includes the following chapters:

- Chapter 3, "Upgrading Oracle Access Manager 11g Release 2 (11.1.2.x.x) Environments"
- Chapter 4, "Upgrading Oracle Adaptive Access Manager 11g Release 2 (11.1.2.x.x) Environments"
- Chapter 5, "Upgrading Oracle Identity Manager 11g Release 2 (11.1.2.x.x) Environments"
- Chapter 6, "Upgrading Oracle Entitlements Server 11g Release 2 (11.1.2.x.x) Environments"
- Chapter 7, "Upgrading Oracle Privileged Account Manager 11g Release 2 (11.1.2.x.x) Environments"
- Chapter 8, "Upgrading Oracle Identity Navigator 11g Release 2 (11.1.2.x.x) Environments"

3

Upgrading Oracle Access Manager 11*g* Release 2 (11.1.2.x.x) Environments

This chapter describes how to upgrade your existing Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0) and 11*g* Release 2 (11.1.2) environments to Oracle Access Management Access Manager (Access Manager) 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

> **Note:** For information about upgrading Oracle Access Management Access Manager on IBM WebSphere, see "Upgrading Access Manager 11g Release 2 (11.1.2.x.x) WebSphere Environments" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

> **Note:** This chapter refers to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2) and 11*g* Release 2 (11.1.2.1.0) environments as 11.1.2.x.x.

This chapter contains the following sections:

- Upgrade Roadmap for Oracle Access Manager
- Reviewing System Requirements and Certification
- Shutting Down Administration Server and Access Manager Managed Server(s)
- Backing Up Oracle Access Manager 11g Release 2 (11.1.2.x.x) Environment
- Upgrading to Oracle WebLogic Server 10.3.6
- Upgrading Access Manager Binaries to 11.1.2.2.0
- Upgrading OAM and OPSS Schemas
- Upgrading Oracle Platform Security Services
- Copying Modified System mbean Configurations
- Shutting Down Administration Server and Access Manager Managed Server(s)
- Upgrading System Configuration
- Starting Administration Server and Access Manager Managed Server(s)
- Upgrading Oracle Access Management Mobile and Service
- Verifying the Upgrade

- Troubleshooting

3.1 Upgrade Roadmap for Oracle Access Manager

Note: If you do not follow the exact sequence provided in this task table, your Oracle Access Manager upgrade may not be successful.

Table 3–1 lists the steps to upgrade Oracle Access Manager 11.1.2.x.x to 11.1.2.2.0.

Table 3–1 Roadmap for Upgrading Access Manager 11.1.2.x.x to 11.1.2.2.0.

Task No.	Task	For More Information
1	Review system requirements and certifications.	See, Reviewing System Requirements and Certification
2	Stop the WebLogic Administration Server and the Access Manager Managed Servers.	See, Shutting Down Administration Server and Access Manager Managed Server(s)
3	Back up the existing Access Manager 11.1.2.x.x environment.	See, Backing Up Oracle Access Manager 11g Release 2 (11.1.2.x.x) Environment
4	Upgrade Oracle WebLogic Server to 10.3.6	See, Upgrading to Oracle WebLogic Server 10.3.6
5	Update the binaries of Access Manager 11.1.2.x.x to 11.1.2.2.0.	See, Upgrading Access Manager Binaries to 11.1.2.2.0
6	Upgrade the Access Manager (OAM) and Oracle Platform Security Services (OPSS) schemas using the Patch Set Assistant.	See, Upgrading OAM and OPSS Schemas
7	Upgrade Oracle Platform Security Services (OPSS). It is highly recommended that you perform this step.	See, Upgrading Oracle Platform Security Services
8	If you are upgrading Access Manager 11.1.2 to 11.1.2.2.0, you must copy the modified system or domain mbean configurations. If you are upgrading Access Manager 11.1.2.1.0 to 11.1.2.2.0, skip this task.	See, Copying Modified System mbean Configurations
9	Stop the Access Manager Managed Server(s) and the WebLogic Administration Server.	See, Shutting Down Administration Server and Access Manager Managed Server(s)
10	Upgrade the system configuration of Access Manager.	See, Upgrading System Configuration
11	Start the WebLogic Administration Server and the Access Manager Managed Server(s).	See, Starting Administration Server and Access Manager Managed Server(s)
12	If you are using the Social Identity feature in Oracle Access Management Mobile and Service, update the Social Identity configuration.	See, Upgrading Oracle Access Management Mobile and Service
13	Verify the Access Manager upgrade.	See, Verifying the Upgrade

3.2 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see Section 2.1, "Reviewing System Requirements and Certification".

3.3 Shutting Down Administration Server and Access Manager Managed Server(s)

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Access Manager Managed Server(s) and the WebLogic Administration Server.

For more information about stopping the servers, see Section 2.8, "Stopping the Servers".

3.4 Backing Up Oracle Access Manager 11*g* Release 2 (11.1.2.x.x) Environment

You must back up your Oracle Access Manager 11.1.2.x.x environment before you upgrade to Access Manager 11.1.2.2.0.

After stopping the servers, back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Access Manager Domain Home directory
- Oracle Access Manager schemas
- MDS schemas
- Audit and any other dependent schemas

For information about backing up the Middleware Home and schemas, see Section 2.2, "Backing up the Existing Environment".

3.5 Upgrading to Oracle WebLogic Server 10.3.6

If you are not using Oracle WebLogic Server 10.3.6, and you must upgrade your existing Oracle WebLogic Server to 10.3.6 by running the WebLogic Server upgrade installer.

For information about upgrading Oracle WebLogic Server to 10.3.6, see Section 2.3, "Upgrading to Oracle WebLogic Server 10.3.6".

3.6 Upgrading Access Manager Binaries to 11.1.2.2.0

To update Access Manager 11.1.2.x.x binaries to Access Manager 11.1.2.2.0, you must use the Oracle Identity and Access Management 11.1.2.2.0 installer. During the procedure, point the Middleware Home to your existing 11.1.2.x.x Oracle Access Manager Middleware Home.

Note: Before upgrading the Access Manager binaries to 11*g* Release 2 (11.1.2.2.0), you must ensure that the OPatch version in *ORACLE_HOME* and *MW_HOME*/oracle_common is 11.1.0.9.9. Different OPatch version might cause patch application failure. If you have upgraded opatch to a newer version, you will have to roll back to version 11.1.0.9.9.

For information about updating the Oracle Identity and Access Management binaries, see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

3.7 Upgrading OAM and OPSS Schemas

After you upgrade Access Manager binaries to 11.1.2.2.0, you must upgrade the OAM and OPSS (Oracle Platform Security Services) schemas by running the Patch Set Assistant. For information about upgrading schemas using Patch Set Assistant, see Section 2.6, "Upgrading Schemas Using Patch Set Assistant".

3.8 Upgrading Oracle Platform Security Services

After you upgrade schemas, it is highly recommended that you upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Access Manager to 11.1.2.2.0. It upgrades the jps-config.xml file and policy stores.

For information about upgrading Oracle Platform Security Services, see Section 2.7, "Upgrading Oracle Platform Security Services"

3.9 Copying Modified System mbean Configurations

If you are upgrading Oracle Access Management Access Manager 11.1.2 to Oracle Access Management Access Manager 11.1.2.2.0, you must copy the modified system or domain mbean configurations from the *OAM_ORACLE_HOME* to the *DOMAIN_HOME*, after you update the Access Manager binaries to 11.1.2.2.0.

Note: If you are upgrading Oracle Access Management Access Manager 11.1.2.1.0 to 11.1.2.2.0, skip this section.

To do this, complete the following steps:

1. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location *$ORACLE_HOME*/common/bin:

   On UNIX: wlst.sh

   On Windows: wlst.cmd

2. Run the following command:

   copyMbeanXmlFiles('*DOMAIN_HOME*','*OAM_ORACLE_HOME*')

   In this command, *DOMAIN_HOME* is the absolute path to the Access Manager WebLogic domain, and *OAM_ORACLE_HOME* is the absolute path to the OAM Oracle home. The second parameter *OAM_ORACLE_HOME* is optional.

For example:

On UNIX:

```
copyMbeanXmlFiles('/Oracle/Middleware/user_projects/domains/base_
domain','/Oracle/Middleware/Oracle_IDM1')
```

On Windows:

```
copyMbeanXmlFiles('C:\\Oracle\\Middleware\\user_projects\domains\\base_
domain','C:\\Oracle\\Middleware\\Oracle_IDM1')
```

3. If the modified system or domain mbean configurations are copied successfully, the following status is displayed on the command line:

```
STATUS: SUCCESS
The mbean xml files have been upgraded to new version.
The original mbean xml is saved in "<domain_directory>/output/upgrade".
Please restart the admin and oam servers.
```

If the `STATUS` shows `SUCCESS`, restart the WebLogic Administration Server and the Access Manager Managed Server(s) by stopping and starting the servers in the following order:

a. Stop the Access Manager Managed Server(s).

For information about stopping Managed Server, see Section 2.8.1, "Stopping the Managed Server(s)".

b. Stop the WebLogic Administration Server.

For information about stopping the WebLogic Administration Server, Section 2.8.2, "Stopping the WebLogic Administration Server".

c. Start the WebLogic Administration Server.

For information about starting the WebLogic Administration Server, see Section 2.9.2, "Starting the WebLogic Administration Server".

d. Start the Access Manager Managed Server(s).

For information about starting Managed Server, see Section 2.9.3, "Starting the Managed Server(s)".

3.10 Shutting Down Administration Server and Access Manager Managed Server(s)

You must shut down the Access Manager Managed Server(s) and the WebLogic Administration Server in order to upgrade system configuration.

For more information about stopping the servers, see Section 2.8, "Stopping the Servers".

3.11 Upgrading System Configuration

After you upgrade to Access Manager binaries to 11.1.2.2.0, you must run the `upgradeConfig()` utility on the machine that hosts Administration Server, to upgrade the system configuration of Access Manager to 11.1.2.2.0. Before you run the `upgradeConfig()` utility, make sure that the Administration Server and the Managed Servers are stopped.

Note: If you are upgrading Access Manager 11.1.2.1.0 to 11.1.2.2.0, then you must do the following before running the `upgradeConfig.sh` command:

1. Go to the directory *ORACLE_HOME*`/common/script_handlers`.
2. Remove all the `.class` files by running the following command:

   ```
   rm *.class
   ```

To upgrade the system configuration of Access Manager, do the following:

1. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location *$ORACLE_HOME*`/common/bin`:

   On UNIX: `./wlst.sh`

   On Windows: `wlst.cmd`

2. Run the following command in offline mode:

   ```
   upgradeConfig("domain_home", "sysdbaUser", "sysdbaPwd",
   "oamSchemaOwner", "oamdbJdbcUrl")
   ```

   In this command,

   - *domain_hom*e is the absolute path to the Access Manager WebLogic domain.
   - *sysdbauser* is the database username having `sysdba` privileges.
   - *sysdbapwd* is the password of the database user having `sysdba` privileges.
   - *oamSchemaOwner* is the database username for OAM schema.
   - *oamdbjdbcUrl* is the JDBC URL to connect to the Access Manager database. The JDBC URL must be in specified in the format `"jdbc:oracle:thin:@<`*server_host*`>:<`*server_port*`>/<`*service_name*`>"`.

   For example:

   On UNIX:

   ```
   upgradeConfig("/Oracle/Middleware/user_projects/domains/base_domain",
   "sys", "pwd", "PREFIX_OAM", "jdbc:oracle:thin:@localhost:1521/orcl")
   ```

   On Windows:

   ```
   upgradeConfig("C:\\Oracle\\Middleware\\user_projects\\domains\\base_
   domain", "sys", "pwd", "PREFIX_OAM",
   "jdbc:oracle:thin:@localhost:1521/orcl")
   ```

3.12 Starting Administration Server and Access Manager Managed Server(s)

Start the WebLogic Administration Server and Access Manager Managed Server(s).

For more information about starting the servers, see Section 2.9, "Starting the Servers".

3.13 Upgrading Oracle Access Management Mobile and Service

If you are using the Social Identity feature in Oracle Access Management Mobile and Service, you must update the Social Identity configuration by running the `msUpgrade()` command. To do this, complete the following steps:

1. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location *$ORACLE_HOME*/common/bin:

   On UNIX: `./wlst.sh`

   On Windows: `wlst.cmd`

2. Run the following command to update the Social Identity configuration:

   ```
   msUpgrade()
   ```

3.14 Verifying the Upgrade

Use the following URL in a web browser to verify that Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0) is running:

```
http://<oam_admin_server_host>:<oam_admin_server_port>/oamconsole
```

3.15 Troubleshooting

This sections describes some of the common issues that you might encounter during the upgrade process, and their workarounds.

Note: For information about the issues that you might encounter during the upgrade process, and their workarounds, see *Oracle Fusion Middleware Release Notes*.

This section contains the following topic:

- Component Version Shows 11.1.1.5.0 After Upgrade

3.15.1 Component Version Shows 11.1.1.5.0 After Upgrade

If you upgraded Oracle Access Manager 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2) first, and then to Access Manager 11.1.2.2.0, the component versions of the packages `oracle.dogwood.top` and `oracle.oam.server` still show 11.1.1.5.0.

The resolve this, you must run the domain updater utility (`com.oracle.cie.domain-update_1.0.0.0.jar`). This step updates the `domain-info.xml`.

To upgrade the necessary Oracle Access Manager packages to 11.1.2.2.0, complete the following steps:

1. Go to the directory *$ORACLE_HOME*/oaam/upgrade. The domain updater utility `com.oracle.cie.domain-update_1.0.0.0.jar` file is located in this directory.

2. Upgrade the package `oracle.dogwood.top` 11.1.1.5.0 to 11.1.2.2.0 by running the following command:

   ```
   java -cp $MW_
   HOME/utils/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
   _1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <DOMAIN_HOME>
   oracle.dogwood.top:11.1.1.5.0,:11.1.2.2.0
   ```

   For example:

   ```
   java -cp
   /scratch/Oracle/Middleware/utils/config/10.3/config-launch.jar:./com.or
   acle.cie.domain-update_1.0.0.0.jar
   ```

```
com.oracle.cie.external.domain.DomainUpdater
/scratch/Oracle/Middleware/user_projects/domains/OAMDomain
oracle.dogwood.top:11.1.1.5.0,:11.1.2.2.0
```

3. Upgrade the package `oracle.oam.server` 11.1.1.5.0 to 11.1.2.2.0 by running the following command:

   ```
   java -cp $MW_
   HOME/utils/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
   _1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <DOMAIN_HOME>
   oracle.oam.server:11.1.1.5.0,:11.1.2.2.0
   ```

   For example:

   ```
   java -cp
   /scratch/Oracle/Middleware/utils/config/10.3/config-launch.jar:./com.or
   acle.cie.domain-update_1.0.0.0.jar
   com.oracle.cie.external.domain.DomainUpdater
   /scratch/Oracle/Middleware/user_projects/domains/OAMDomain
   oracle.oam.server:11.1.1.5.0,:11.1.2.2.0
   ```

4

Upgrading Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.x.x) Environments

This chapter describes how to upgrade Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.1.0) and 11*g* Release 2 (11.1.2) environments to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

Note: For information about upgrading Oracle Adaptive Access Manager on IBM WebSphere, see "Upgrading Oracle Adaptive Access Manager on IBM WebSphere" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

Note: This chapter refers to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2) and 11*g* Release 2 (11.1.2.1.0) environments as 11.1.2.x.x.

This chapter includes the following sections:

- Section 4.1, "Upgrade Roadmap for Oracle Adaptive Access Manager"
- Section 4.2, "Reviewing System Requirements and Certification"
- Section 4.3, "Shutting Down Administration Server and Managed Servers"
- Section 4.4, "Backing Up Oracle Adaptive Access Manager 11.1.2.x.x"
- Section 4.5, "Optional: Upgrading Oracle WebLogic Server"
- Section 4.6, "Updating Oracle Adaptive Access Manager Binaries to 11.1.2.2.0"
- Section 4.7, "Upgrading OAAM, MDS, IAU, and OPSS Schemas"
- Section 4.8, "Upgrading Oracle Platform Security Services"
- Section 4.9, "Starting the Servers"
- Section 4.10, "Redeploying the Applications"
- Section 4.11, "Verifying the Upgrade"

4.1 Upgrade Roadmap for Oracle Adaptive Access Manager

Note: If you do not follow the exact sequence provided in this task table, your Oracle Adaptive Access Manager upgrade may not be successful.

Table 4–1 lists the steps to upgrade Oracle Adaptive Access Manager.

Table 4–1 Roadmap for Upgrading Oracle Adaptive Access Manager 11.1.2.x.x to 11.1.2.2.0.

Sl No	Task	For More Information
1	Review system requirements and certifications.	See, Reviewing System Requirements and Certification
2	Stop the WebLogic Administration Server and the Oracle Adaptive Access Manager Managed Server(s) before you start the upgrade process.	See, Shutting Down Administration Server and Managed Servers
3	Back up your existing Oracle Adaptive Access Manager 11.1.2.x.x Environment.	See, Backing Up Oracle Adaptive Access Manager 11.1.2.x.x
4	Upgrade Oracle WebLogic Server to 10.3.6, if necessary.	See, Optional: Upgrading Oracle WebLogic Server
5	Update the Oracle Adaptive Access Manager 11.1.2.x.x binaries to 11.1.2.2.0.	See, Updating Oracle Adaptive Access Manager Binaries to 11.1.2.2.0
6	Upgrade the OAAM, MDS, IAU, and OPSS Schemas using Patch Set Assistant.	See, Upgrading OAAM, MDS, IAU, and OPSS Schemas
7	Upgrade the Oracle Platform Security Services.	See, Upgrading Oracle Platform Security Services
8	Start the WebLogic Administration Server and Oracle Adaptive Access Manager Managed Server(s).	See, Starting the Servers
9	If you are upgrading Oracle Adaptive Access Manager 11.1.2 to 11.1.2.2.0, you must redeploy the applications after you start the servers.	See, Redeploying the Applications
10	Verify the Oracle Adaptive Access Manager upgrade.	See, Verifying the Upgrade

4.2 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see Section 2.1, "Reviewing System Requirements and Certification".

4.3 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the WebLogic Administration Server and the Oracle Adaptive Access Manager Managed Servers.

For more information about stopping the WebLogic Administration Server and the Managed Servers, see Section 2.8, "Stopping the Servers".

4.4 Backing Up Oracle Adaptive Access Manager 11.1.2.x.x

You must back up your Oracle Adaptive Access Manager 11.1.2.x.x environment before you upgrade to Oracle Adaptive Access Manager 11.1.2.2.0.

After stopping the servers, you must back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Oracle Adaptive Access Manager Domain Home directory
- Oracle Adaptive Access Manager schema
- IAU schema, if it is part of any of your Oracle Adaptive Access Manager 11.1.2.x.x schema
- MDS schema

For more information about backing up the Middleware Home and the schemas, see Section 2.2, "Backing up the Existing Environment".

4.5 Optional: Upgrading Oracle WebLogic Server

Note: Upgrading Oracle WebLogic Server is not mandatory. However, Oracle recommends that you upgrade Oracle WebLogic Server to 10.3.6.

You can upgrade your existing WebLogic Server to Oracle WebLogic Server 10.3.6 if you are not using Oracle WebLogic Server 10.3.6.

For information about upgrading Oracle WebLogic Server to 10.3.6, see Section 2.3, "Upgrading to Oracle WebLogic Server 10.3.6".

4.6 Updating Oracle Adaptive Access Manager Binaries to 11.1.2.2.0

To update the Oracle Adaptive Access Manager 11.1.2.x.x binaries to 11.1.2.2.0, you must use the Oracle Identity and Access Management 11.1.2.2.0 Installer. During the procedure, point the Middleware Home to your existing 11.1.2.x.x Middleware Home. Your Oracle Home is upgraded from 11.1.2.x.x to 11.1.2.2.0.

For information about updating the Oracle Adaptive Access Manager binaries to 11.1.2.2.0, see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

4.7 Upgrading OAAM, MDS, IAU, and OPSS Schemas

You must upgrade the following schemas using Patch Set Assistant:

- OAAM schema
- MDS schema
- OPSS schema
- IAU schema (You must upgrade Audit schema (IAU) only if it is part of your 11.1.2.x.x schemas.

> **Note:** When upgrading schemas using Patch Set Assistant, you must select **OAAM** or **OAAM_PARTN** as appropriate, and provide details on all screens to complete the upgrade.

For information about upgrading schemas using Patch Set Assistant, see Section 2.6, "Upgrading Schemas Using Patch Set Assistant".

4.8 Upgrading Oracle Platform Security Services

After you upgrade schemas, you must upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Adaptive Access Manager to 11.1.2.2.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see Section 2.7, "Upgrading Oracle Platform Security Services".

4.9 Starting the Servers

Start the WebLogic Administration Server and the Oracle Adaptive Access Manager Managed Server(s).

For information about starting the WebLogic Administration Server and the Managed Servers, see Section 2.9, "Starting the Servers".

4.10 Redeploying the Applications

If you are upgrading Oracle Adaptive Access Manager 11.1.2 to 11.1.2.2.0, you must redeploy changes to the applications in the domain. Redeploy your 11.1.2 application on the Oracle Adaptive Access Manager 11.1.2.2.0 servers.

You can redeploy the application using command line or using the WebLogic Administration console. Complete the following steps described in one of the following sections to redeploy applications:

- Redeploying Applications Using Command Line
- Redeploying Applications Using WebLogic Administration Console

Redeploying Applications Using Command Line

To redeploy applications on Oracle Adaptive Access Manager 11.1.2.2.0 servers using command line, do the following:

1. Launch the WebLogic Scripting Tool (WLST) by running the following command from the location *IAM_HOME*`/common/bin`:

   On UNIX: `./wlst.sh`

On Windows: `wlst.cmd`

2. Connect to the Administration Server using the following command:

   `connect('weblogic-username','weblogic-password','weblogic-url')`

   For example:

   `connect('wlsuser','wlspassword','localhost:7001')`

3. Stop the applications by running the following commands:

   - `stopApplication('oaam_admin')`
   - `stopApplication('oaam_server')`

   Note: If you have Oracle Adaptive Access Manager Offline Server in your setup, run the `stopApplication()` command to stop `'oaam_offline'` too.

4. Redeploy the applications by running the following commands:

   - `redeploy('oracle.oaam.extensions')`
   - `redeploy('oaam_admin')`
   - `redeploy('oaam_server')`

   Note: If you have Oracle Adaptive Access Manager Offline Server in your setup, run the `redeploy()` command to redeploy applications on `'oaam_offline'` too.

5. Start the applications by running the following commands:

   - `startApplication('oaam_admin')`
   - `startApplication('oaam_server')`

   Note: If you have Oracle Adaptive Access Manager Offline Server in your setup, run the `startApplication()` command to stop `'oaam_offline'` too.

6. Exit the WLST console using the `exit()` command.

For more information about using the `redeploy` command, see "redeploy" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Redeploying Applications Using WebLogic Administration Console

To redeploy applications on Oracle Adaptive Access Manager 11.1.2.2.0 servers using the WebLogic Administration console, do the following

1. Log in to the WebLogic Administration console using the following URL:

   `http://admin_host:admin_port/console`

2. Go to the **Deployments** tab.
3. Click **lock and Edit** on the left panel.
4. Select **oaam_extension_library**.

5. Click **Update.**
6. The console shows the location of the `.ear` file. Confirm if that is the correct location of the `.ear` file that you wish to deploy; Otherwise, change the location.
7. Click **Finish**.
8. When the deployment is completed, click **Release configuration**.
9. Repeat the procedure for `OAAM_ADMIN`, `OAAM_SERVER`, and `OAAM_OFFLINE` as applicable.

4.11 Verifying the Upgrade

To verify the Oracle Adaptive Access Manager upgrade, do the following:

- Verify the log file at the location *`MW_HOME`*`/oracle_common/upgrade/logs` to ensure that the upgrade was successful.
- Verify the version of the OAAM schema by connecting to the OAAM schema as *`OAAM_schema_user`*, and running the following query:

  ```
  select version,status,upgraded from schema_version_registry where
  owner=<SCHEMA_NAME>;
  ```

  Ensure that the version number is 11.1.2.2.0.
- Log in to the OAAM Administration console using the following URL:

  ```
  http://oaam.example.com:<oaam_port>/oaam_admin
  ```

  Verify if the version number of Oracle Adaptive Access Manager is 11.1.2.2.0.

5

Upgrading Oracle Identity Manager 11*g* Release 2 (11.1.2.x.x) Environments

This chapter describes how to upgrade Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) and 11*g* Release 2 (11.1.2) environments to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

Note: For information about upgrading Oracle Identity Manager on IBM WebSphere, see "Upgrading Oracle Identity Manager on IBM WebSphere" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

Note: This chapter refers to Oracle Identity Manager 11*g* Release 2 (11.1.2) and 11*g* Release 2 (11.1.2.1.0) environments as 11.1.2.x.x.

This chapter includes the following sections:

- Upgrade Roadmap for Oracle Identity Manager
- Pre-Upgrade Steps
- Upgrading the Oracle Home and Database Schemas
- Upgrading the Oracle Identity Manager Middle Tier
- Upgrading Other Oracle Identity Manager Installed Components
- Post-Upgrade Steps

5.1 Upgrade Roadmap for Oracle Identity Manager

The procedure for upgrading Oracle Identity Manager 11.1.2.x.x to 11.1.2.2.0 involves the following high-level steps

1. **Pre-Upgrade Steps**: This step involves the necessary pre-upgrade tasks like reviewing system requirements and certification, generating the pre-upgrade report, analyzing the report and performing the necessary pre-upgrade tasks described in the report, backing up the existing 11.1.2.x.x environment.
2. **Upgrading the Oracle Home and Database Schemas**: This step involves tasks like upgrading Oracle WebLogic Server, upgrading Oracle SOA Suite, upgrading Oracle Identity Manager binaries, upgrading Oracle Platform Security Services, upgrading JRF, upgrading Oracle Identity Manager schema.

3. **Upgrading the Oracle Identity Manager Middle Tier**: This step involves upgrading Oracle Identity Manager middle tier.
4. **Upgrading Other Oracle Identity Manager Installed Components**: This step involves tasks like upgrading Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manger to 11.1.2.2.0.
5. **Post-Upgrade Steps**: This step involves any post-upgrade tasks, and the steps to verify the upgrade.

Table 5–1 lists the steps to upgrade Oracle Identity Manager 11.1.2.x.x to 11.1.2.2.0.

Table 5–1 Roadmap for Upgrading Oracle Identity Manager 11.1.2.x.x to 11.1.2.2.0

Sl No	Task	For More Information
	Pre-Upgrade Steps	
1	Review the changes in the features of Oracle Identity Manager 11.1.2.2.0.	See, Feature Comparison
2	Review system requirements and certifications.	See, Reviewing System Requirements and Certification
3	Generate the pre-upgrade report, analyze the information provided in the report, and perform the necessary tasks described in the report before you proceed with the upgrade process.	See, Generating and Analyzing the Pre-Upgrade Report
4	Back up the existing Oracle Identity Manager 11.1.2.x.x environment.	See, Backing Up Oracle Identity Manager 11.1.2.x.x Environment
5	Set the JVM properties for the Oracle Identity Manager Server(s) using the WebLogic Administration console.	See, Setting JVM Properties for Oracle Identity Manager Server(s)
6	Stop the Node Manager, WebLogic Administration Server, Oracle SOA Suite Managed Server(s), and the Oracle Identity Manager Managed Server(s).	See, Shutting Down Node Manager, Administration Server and Managed Server(s)
	Upgrading the Oracle Home and Database Schemas	
7	If you are not using Oracle WebLogic Server 10.3.6, and you must upgrade Oracle WebLogic Server to 10.3.6.	See, Upgrading Oracle WebLogic Server to 10.3.6
8	Upgrade your existing Oracle SOA Suite to Oracle SOA Suite 11*g* Release 1 (11.1.1.7.0).	See, Upgrading Oracle SOA Suite to 11.1.1.7.0
9	Update the Oracle Identity Manager 11.1.2.x.x binaries to 11.1.2.2.0.	See, Upgrading Oracle Identity Manager Binaries to 11.1.2.2.0
10	Upgrade the OPSS, MDS, OIM, ORASDPM, and SOAINFRA schemas using the Patch Set Assistant.	See, Upgrading Schemas
11	Upgrade the Oracle Platform Security Services (OPSS) by running the WLST command `upgradeOpss`.	See, Upgrading Oracle Platform Security Services
12	Upgrade the Java Required Files (JRF).	See, Upgrading Java Required Files (JRF)

Table 5–1 (Cont.) Roadmap for Upgrading Oracle Identity Manager 11.1.2.x.x to

Sl No	Task	For More Information
	Upgrading the Oracle Identity Manager Middle Tier	
13	Start the WebLogic Administration Server, and the SOA Managed Server(s), if not already started.	See, Starting Administration Server and SOA Managed Server(s)
14	Upgrade the existing Oracle Identity Manager middle tier.	See, Upgrading Oracle Identity Manager Middle Tier
15	Restart the WebLogic Administration Server, Oracle Identity Manager Managed Server(s), and the SOA Managed Server(s).	See, Restarting all the Servers
	Upgrading Other Oracle Identity Manager Installed Components	
16	Upgrade the Oracle Identity Manager Design Console to 11.1.2.2.0.	See, Upgrading Oracle Identity Manager Design Console
17	Upgrade the Oracle Identity Manager Remote Manager to 11.1.2.2.0.	See, Upgrading Oracle Identity Manager Remote Manager
	Post-Upgrade Steps	
18	Perform all mandatory post-upgrade steps.	See, Performing the Post-Upgrade Tasks
19	Verify the Oracle Identity Manager upgrade.	See, Verifying the Upgrade

5.2 Pre-Upgrade Steps

This section describes all the pre-upgrade steps that you must complete before you start upgrading the Oracle Identity Manager 11.1.2.x.x environment. This section includes the following topics:

- Feature Comparison
- Reviewing System Requirements and Certification
- Generating and Analyzing the Pre-Upgrade Report
- Backing Up Oracle Identity Manager 11.1.2.x.x Environment
- Setting JVM Properties for Oracle Identity Manager Server(s)
- Shutting Down Node Manager, Administration Server and Managed Server(s)

5.2.1 Feature Comparison

Table 5–2 lists the key differences in functionality between Oracle Identity Manager 11*g* Release 2 (11.1.2), 11*g* Release 2 (11.1.2.1.0), and 11*g* Release 2 (11.1.2.2.0).

Table 5–2 Features Comparison

Oracle Identity Manager 11.1.2 and/or 11.1.2.1.0	Oracle Identity Manager 11.1.2.2.0
Oracle Identity Manager 11.1.2 provided Identity Attestation to periodically review users access. For advanced access review capabilities such as role or data owner certification, OIM 11.1.2 had to be integrated with Oracle Identity Analytics (OIA) to leverage the advanced access review capabilities that OIA provided.	In Oracle Identity Manager 11.1.2.1.0 and 11.1.2.2.0, the advanced access review capabilities of OIA are converged into OIM to provide a complete identity governance platform that enables an enterprise to do enterprise grade access request, provisioning, and access review from a single product. After upgrading to Oracle Identity Manager 11.1.2.2.0, you can use the new access review capabilities. This feature is disabled by default. Therefore, you must ensure that you have relevant licenses before enabling this new feature.
In Oracle Identity Manager 11.1.2.1.0, certification was introduced and the workflow supported one level of access review in each phase.	Certification workflow in 11.1.2.2.0 enables business to define more robust processes for compliance, enabling more granular oversight of "who has access to what". Certification reviews can mirror access request workflow, where they can be reviewed or approved by multiple sets of business and IT owners before they are deemed complete in each phase. This ensures improved visibility of user access privileges, and all review decisions are captured in a comprehensive audit trail that is recorded live during the certification as well as in reports.
In Oracle Identity Manager 11.1.2 and 11.1.2.1.0, users are assigned to organizations by specifying an organization name in the `Organization` attribute of the user details. This is a static organization membership.	In Oracle Identity Manager 11.1.2.2.0, in addition to the existing feature, you can dynamically assign users to organizations based on user-membership rules, which you can define in the **Members** tab of the organization details page. All users who satisfy the user-membership rule are dynamically associated with the organization, irrespective of the organization hierarchy the users statically belong to. With this new capability, a user can gain membership of one home organization via static membership and multiple secondary organizations via user-membership rules that are dynamically evaluated.
Oracle Identity Manager 11.1.2 and 11.1.2.1.0 uses the Fusion Fx skin which provides a rich look and feel.	Oracle Identity Manager 11.1.2.2.0 uses Skyros skin. This is a light-weight skin that uses fewer background images and does not need gradients. This ensures that the UI renders allot faster and UI skinning becomes easier. After you upgrade to OIM 11.1.2.2.0, the Skyros skin will be enabled by default. There is also an option to revert back to the Fusion Fx skin post upgrade.

Table 5–2 (Cont.) Features Comparison

Oracle Identity Manager 11.1.2 and/or 11.1.2.1.0	Oracle Identity Manager 11.1.2.2.0
In Oracle Identity Manager 11.1.2 and 11.1.2.1.0, you had to explicitly request for an account and ensure it was provisioned before you could request for an entitlement in that account. If you requested for an entitlement and did not have the corresponding account, the request fails.	In Oracle Identity Manager 11.1.2.2.0, entitlement and account dependency are introduced in the OIM catalog. After you upgrade to Oracle Identity Manager 11.1.2.2.0, this new feature allows you to request for the following: ■ Entitlements even if you do not have the corresponding account. ■ Entitlements for a specific account in addition to the primary account, if you have multiple account instances in the same application.
In Oracle Identity Manager 11.1.2, catalog was introduced to provide meaningful and contextual information to end users during the request and access review. The catalog allows you to associate meaningful metadata against any request able entity.	In Oracle Identity Manager 11.1.2.2.0, in addition to the catalog metadata, you can enable the display of hierarchical attributes of entitlements to requesters, approvers, and certifiers to view additional details of entitlements (hierarchical attributes) in the catalog detail screen. The additional details of entitlements is called technical glossary. The technical glossary is displayed in a tree structure.
The catalog in Oracle Identity Manager 11.1.2 and 11.1.2.1.0 supports simple entitlements when you request for an entitlement. A simple entitlement has a single attribute.	The catalog in Oracle Identity Manager 11.1.2.2.0 supports request for complex entitlements. A complex entitlement is an entitlement with more than one attribute. These attributes will be presented in an Entitlement Form on the request check out page.
In Oracle Identity Manager 11.1.2 and 11.1.2.1.0, you cannot save a request in draft mode. If you cannot complete the access request, you must start the entire request process from the beginning when you resume.	In Oracle Identity Manager 11.1.2.2.0, you can use the draft request feature and save any request as a draft at any point of time. Once a request is saved as a draft, you can return to the self service console whenever required and continue with the data that you provided earlier.
The data rich and stateful nature of the Oracle Identity Manager causes state-related data to accumulate which in turn slows down the deployment. OIM customers are encouraged to run the archive and purge scripts frequently. The archive and purge utilities in Oracle Identity Manager 11.1.2 and 11.1.2.1.0 are command line based, and requires you to navigate through an interactive wizard. This requires manual intervention each time archive and purge is run.	In Oracle Identity Manager 11.1.2.2.0, real time continuous archive and purge utilities are available. You can define the archive and purge thresholds and parameters, and schedule the utilities to run automatically in periodic intervals.
In Oracle Identity Manager 11.1.2 and 11.1.2.1.0, Diagnostic Dashboard is used to validate pre installation and post installation requirements. Diagnostic Dashboard is a standalone web application that runs on the application server. It also provides very rudimentary mechanisms to trace and diagnose orchestration errors.	In Oracle Identity Manager 11.1.2.2.0, you can use the Fusion Middleware Enterprise Manager console to view the configuration and state of operations in Oracle Identity Manager.

5.2.2 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see Section 2.1, "Reviewing System Requirements and Certification".

5.2.3 Generating and Analyzing the Pre-Upgrade Report

You must run the pre-upgrade report utility before you begin the upgrade process, and address all the issues listed as part of this report with the solution provided in the report. The pre-upgrade report utility analyzes your existing Oracle Identity Manager 11.1.2.x.x environment, and provides information about the mandatory prerequisites that you must complete before you upgrade the existing Oracle Identity Manager environment.

The information in the pre-upgrade report for 11.1.2 starting point is related to challenge questions localization, authorization feature data upgrade, event handlers that are affected by upgrade, and mandatory database components or settings.

The information in the pre-upgrade report for 11.1.2.1.0 starting point is related to challenge questions localization, authorization feature upgrade, mandatory database components or settings, cyclic groups in LDAP that need to be removed, certification records processed during the upgrade, and the potential application instance creation issues.

Note: Run this report until no pending issues are listed in the report.

It is important to address all the issues listed in the pre-upgrade report, before you can proceed with the upgrade, as upgrade might fail if the issues are not fixed.

To generate and analyze the pre-upgrade report, complete the tasks described in the following sections:

- Obtaining Pre-Upgrade Report Utility
- Generating the Pre-Upgrade Report
- Analyzing the Pre-Upgrade Report

5.2.3.1 Obtaining Pre-Upgrade Report Utility

You must download the pre-upgrade utility from Oracle Technology Network (OTN). The utility is available in two zip files named `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002`, along with `ReadMe.doc` at the following location on My Oracle Support:

My Oracle Support document ID 1599043.1

The `ReadMe.doc` contains information about how to generate and analyze the pre-upgrade reports.

5.2.3.2 Generating the Pre-Upgrade Report

To generate the pre-upgrade report for Oracle Identity Manager 11.1.2.x.x upgrade, do the following:

1. Create a directory at any location and extract the contents of `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002` in the newly created directory.
2. Create a directory where pre-upgrade reports need to be generated. For example, name the directory *`OIM_preupgrade_reports`*.
3. Go to the directory where you extracted `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002`, and open the `preupgrade_report_input.properties` file in a text editor. Update the properties file by specifying the appropriate values for the parameters listed in Table 5–3:

Table 5–3 Parameters to be Specified in the preupgrade_report_input.properties File

Parameter	Description
`oim.targetVersion`	Specify `11.1.2.2.0` for this parameter, as `11.1.2.2.0` is the target version for which pre-upgrade utility needs to be run.
`oim.jdbcurl`	Specify the JDBC URL for Oracle Identity Manager in the following format: *<host>:<port>/<service_name>*
`oim.oimschemaowner`	Specify the name of the OIM schema owner.
`oim.mdsjdbcurl`	Specify the MDS JDBC URL in the following format: *<host>:<port>/<service_name>*
`oim.mdsschemaowner`	Specify the name of the MDS schema owner.
`oim.databaseadminname`	Specify the user with DBA privilege. For example, `sys as sysdba`.
`oim.outputreportfolder`	Specify the absolute path to the directory that you created in step-2 (directory with name *`OIM_preupgrade_reports`*), where the pre-upgrade reports need to be generated. Make sure that the output report folder has read and write permissions.
`oim.oimhome`	Specify the absolute path to the OIM Home.
`oim.domain`	Specify the absolute path to the Oracle Identity Manager domain home. For example: `/Middleware/user_projects/domains/base_domain`
`oim.wlshome`	Specify the absolute path to the WebLogic Server home. For example: `/Middleware/wlserver_10.3`

4. Set the environment variables `JAVA_HOME`, `MW_HOME`, `WL_HOME`, and `OIM_HOME` by running the following commands:

   On UNIX:

   ```
   export JAVA_HOME=<absolute_path_to_jdk_location>

   export MW_HOME=<absolute_path_to_middleware_home>

   export OIM_HOME=<absolute_path_to_middleware_home>/Oracle_IDM1/
   ```

   On Windows:

```
set JAVA_HOME="<absolute_path_to_jdk_location>"

set MW_HOME="<absolute_path_to_middleware_home>"

set OIM_HOME="<absolute_path_to_middleware_home>\Oracle_IDM1\"
```

5. Run the following command from the location where you extracted the contents of `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002`.
   - **On UNIX**:

     ```
     sh generatePreUpgradeReport.sh
     ```

   - **On Windows**:

     ```
     generatePreUpgradeReport.bat
     ```

6. Provide the details when the following is prompted:
   - **OIM Schema Password**

     You must enter the password of the OIM schema.

   - **DBA Password**

     You must enter the password of the Database Administrator.

7. The reports are generated as HTML pages at the location you specified for the parameter `oim.outputreportfolder` in the `preupgrade_report_input.properties` file. The logs are stored in the log file `preUpgradeReport<time>.log` in the folder `logs` at the same location.

   The following are the reports generated by the pre-upgrade report utility:

   Pre-Upgrade Reports Generated for 11.1.2 Starting Point

   - `index.html`
   - `ChallengeQuesPreUpgradeReport.html`
   - `DomainReassocAuthorization.html`
   - `EVENT_HANDLERPreUpgradeReport.html`
   - `ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html`
   - `ORACLE_ONLINE_PURGEPreUpgradeReport.html`
   - `PasswordPolicyPreUpgradeReport.html`
   - `UDFPreUpgradeReport.html`
   - `WLSMBEANPreUpgradeReport.html`

   Pre-Upgrade Reports Generated for 11.1.2.1.0 Starting Point

   - `index.html`
   - `CertificationUpgradeReport.html`
   - `ChallengeQuesPreUpgradeReport.html`
   - `CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html`
   - `DomainReassocAuthorization.html`
   - `ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html`
   - `ORACLE_ONLINE_PURGEPreUpgradeReport.html`
   - `PasswordPolicyPreUpgradeReport.html`

- PROVISIONINGPreUpgradeReport.html
- UDFPreUpgradeReport.html
- WLSMBEANPreUpgradeReport.html

5.2.3.3 Analyzing the Pre-Upgrade Report

After you generate the pre-upgrade report, you must review each of the reports, and perform all the tasks described in them. If you do not perform the mandatory tasks described in the report before you upgrade, the upgrade might fail.

Table 5–4 lists all the pre-upgrade reports, describes what information each report contains, and provides links to the detailed description of each report.

Table 5–4 Description of Pre-Upgrade Reports

Sl No	HTML Report Name	Generated for the Starting Points	Description	For Detailed Description
1	index.html	11.1.2 11.1.2.1.0	This report provides links to all the other reports generated by the pre-upgrade report utility. It also states that you must run the pre-upgrade report utility till no pending issues are listed in this report.	See, Description of index.html Report
2	CertificationUpgradeReport.html	11.1.2.1.0	This report lists the certification records processed during the upgrade of snapshot data. You must review the information provided in this report.	See, Description of CertificationUpgradeReport.html Report

Table 5–4 (Cont.) Description of Pre-Upgrade Reports

Sl No	HTML Report Name	Generated for the Starting Points	Description	For Detailed Description
3	`ChallengeQuesPreUpgradeReport.html`	11.1.2 11.1.2.1.0	This report provides information about upgrading localized challenge questions data. This report is generated for Oracle Identity Manager upgrade on WebLogic Server only. When you upgrade Oracle Identity Manager 11.1.2.x.x to 11.1.2.2.0, the existing localization data for challenge questions is lost. Therefore, before proceeding with the upgrade process, you must backup the existing localized challenge questions data. After you upgrade to Oracle Identity Manager 11.1.2.2.0, you must perform the tasks described in this report. If you have already migrated the localized challenge questions data per new localization model provided in Oracle Identity Manager 11*g* Release 2 (11.1.2.0.11) or (11.1.2.1.3), then skip the tasks described in this report.	See, Description of ChallengeQuesPreUpgradeReport.html Report
4	`CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html`	11.1.2.1.0	This report detects and displays the list of cyclic groups in LDAP. Cyclic groups in LDAP directory are not supported in 11.1.2.2.0. Therefore, you must remove the cyclic dependency from existing Oracle Identity Manager setup and reconcile data from LDAP to Oracle Identity Manager Database. The procedure for doing this is described in the report.	See, Description of CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html Report

Table 5–4 (Cont.) Description of Pre-Upgrade Reports

Sl No	HTML Report Name	Generated for the Starting Points	Description	For Detailed Description
5	DomainReassocAuthorization.html	11.1.2 11.1.2.1.0	This report lists the checks executed for authorization feature data upgrade. It checks if the Oracle Identity Manager is reassociated with the DB-based policy store. Review the table that lists the checks executed and the status of the checks.	See, Description of DomainReassocAuthorization.html Report
6	EVENT_HANDLERPreUpgradeReport.html	11.1.2	This report lists the event handlers that are affected by the upgrade. Review the details in the report, and perform any necessary resolution tasks specified in the report.	See, Description of EVENT_HANDLERPreUpgradeReport.html Report
7	ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html	11.1.2 11.1.2.1.0	This report provides the status of the mandatory database components or settings for Oracle Identity Manager upgrade. Verify the installation or setup status for each of the mandatory component or setting. If any of the component or setting is not setup correctly, follow the recommendations provided in the report to fix them.	See, Description of ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html Report
8	ORACLE_ONLINE_PURGEPreUpgradeReport.html	11.1.2 11.1.2.1.0	This report lists the pre-requisites for Online Purge that needs to be addressed before you proceed with the upgrade. This report will not be generated if there is no action item related to purge.	See, Description of ORACLE_ONLINE_PURGEPreUpgradeReport.html Report

Table 5–4 (Cont.) Description of Pre-Upgrade Reports

Sl No	HTML Report Name	Generated for the Starting Points	Description	For Detailed Description
9	`PasswordPolicyPreUpgradeReport.html`	11.1.2	This report lists the potential upgrade issues for password policies. If you are relying on 9.1.x.x password policy model, you must update to new password policies, as 9.1.x.x password policy model is not supported in 11.1.2.2.0. Review the report and assign the password policies listed in the report to appropriate organization(s).	See, Description of PasswordPolicyPreUpgradeReport.html Report

Table 5–4 (Cont.) Description of Pre-Upgrade Reports

Sl No	HTML Report Name	Generated for the Starting Points	Description	For Detailed Description
10	PROVISIONINGPreUpgradeReport.html	11.1.2.1.0	This report lists the potential application instance creation issues. It provides information about the following: ■ Provisioning Configuration ■ Entitlement Configuration ■ Access Policy Configuration ■ List of Resource Objects without Process Form ■ List of Resource Objects without ITResource field Type in Process Form ■ List of Resource Objects with multiple ITResource Lookup fields in Process Form ■ List of Access Policies without ITResource value set in default policy data ■ List of Access Policies with Revoke If No Longer Applies flag unchecked ■ List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value Review all the sections in the report and perform necessary tasks.	See, Description of PROVISIONINGPreUpgradeReport.html Report
11	UDFPreUpgradeReport.html	11.1.2 11.1.2.1.0	This report lists the tasks that you must perform prior to upgrade to ensure that the User Defined Fields (UDFs) are upgraded seamlessly. Perform all the necessary tasks described in this report.	See, Description of UDFPreUpgradeReport.html Report

Table 5–4 (Cont.) Description of Pre-Upgrade Reports

Sl No	HTML Report Name	Generated for the Starting Points	Description	For Detailed Description
12	WLSMBEANPreUpgradeReport.html	11.1.2 11.1.2.1.0	This report lists the .jar files present in the WebLogic. mbean paths that need to be deleted before performing middle tier upgrade. Review the information provided in this report, and perform necessary action.	See, Description of WLSMBEANPreUpgradeReport.html Report

5.2.3.3.1 Description of index.html Report The report index.html is generated for both 11.1.2 and 11.1.2.1.0 starting points. This is the index page that contains links to the other reports.

Table 5–5 lists the reports displayed in index.html for the starting point 11.1.2, and their corresponding HTML report names.

Table 5–5 Reports Listed in index.html for Starting Point 11.1.2

Report Name in index.html	Corresponding HTML Report
Installation Status of Mandatory Database Components	ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html
Installation Status of UDF	UDFPreUpgradeReport.html
Status of Mandatory deletion of OIM Authenticator Jar(s)	WLSMBEANPreUpgradeReport.html
Event Handlers affected during upgrade	EVENT_HANDLERPreUpgradeReport.html
Domain Reassociation report	DomainReassocAuthorization.html
Challenge Questions report	ChallengeQuesPreUpgradeReport.html
Potential upgrade issues for Password Policies	PasswordPolicyPreUpgradeReport.html
Prerequisites for Online Purge	ORACLE_ONLINE_PURGEPreUpgradeReport.html

Table 5–6 lists the reports displayed in index.html for the starting point 11.1.2.1.0, and their corresponding HTML report names.

Table 5–6 Reports Listed in index.html for Starting Point 11.1.2.1.0

Report Name in index.html	Corresponding HTML Report
Installation Status of Mandatory Database Components	ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html
Installation Status of UDF	UDFPreUpgradeReport.html

Table 5–6 (Cont.) Reports Listed in index.html for Starting Point 11.1.2.1.0

Report Name in index.html	Corresponding HTML Report
Status of Mandatory deletion of OIM Authenticator Jar(s)	`WLSMBEANPreUpgradeReport.html`
Certification Report	`CertificationUpgradeReport.html`
Domain Reassociation report	`DomainReassocAuthorization.html`
Challenge Questions report	`ChallengeQuesPreUpgradeReport.html`
List of cyclic groups in LDAP directory	`CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html`
List of potential app instance creation issues	`PROVISIONINGPreUpgradeReport.html`
Potential upgrade issues for Password Policies	`PasswordPolicyPreUpgradeReport.html`
Prerequisites for Online Purge	`ORACLE_ONLINE_PURGEPreUpgradeReport.html`

5.2.3.3.2 Description of CertificationUpgradeReport.html Report

The report `CertificationUpgradeReport.html` lists the certification records processed during the upgrade of snapshot data. This report displays a table that contains the certification record ID, column name, current value, and the new value. Review the information provided in the table.

5.2.3.3.3 Description of ChallengeQuesPreUpgradeReport.html Report

The report `ChallengeQuesPreUpgradeReport.html` is generated for both 11.1.2 and 11.1.2.1.0 starting points.

When you upgrade Oracle Identity Manager 11.1.2.x.x to 11.1.2.2.0, the existing localization data for challenge questions is lost as it is not upgrade-safe. Therefore, before you upgrade to Oracle Identity Manager 11.1.2.2.0, you must backup the existing localized challenge questions data.

After you upgrade to 11.1.2.2.0, perform the tasks described in this report to localize challenge questions. Follow the instructions in the section applicable for your starting point.

> **Note:** If you have already migrated the localized challenge questions data per localization model provided in Oracle Identity Manager 11*g* Release 2 (11.1.2.0.11) or (11.1.2.1.3), ignore the tasks described in this report.

5.2.3.3.4 Description of CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html Report

The report `CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html` provides information about the Cyclic groups in LDAP directory.

Oracle Identity Manager 11.1.2.2.0 does not support cyclic groups in the LDAP directory. Therefore, you must remove any cyclic dependency from your existing setup and reconcile data from LDAP to Oracle Identity Manager Database, before you proceed with the upgrade.

For more information about removing the cyclic groups dependent on LDAP, see Removing Cyclical Groups Dependent on LDAP and Reconciling Data From LDAP to

OIM Database. The procedure for removing cyclic groups is also described in this report.

Removing Cyclical Groups Dependent on LDAP and Reconciling Data From LDAP to OIM Database

If the LDAP in your existing Oracle Identity Manager environment has cyclic groups loaded, you must remove the cyclic groups by doing the following:.

1. Use JEXplorer or Softerra LDAP Administrator and navigate to the cyclic groups.
2. Look for **uniquemember** attribute.
3. Remove all values from the attribute.
4. Save the group.
5. Reconcile the data from LDAP to Oracle Identity Manager Database by running the following command:

   On UNIX: `LDAPConfigPostSetup.sh`

   On Windows: `LDAPConfigPostSetup.bat`

Example Scenario

If you have cyclic group dependency between two groups: Group1 and Group2, do the following to remove cyclic dependency:

1. Connect to LDAP using JEXplorer or Softerra LDAP.
2. Go to the group container of Group1.
3. Go to the **uniquemember** attribute under Group1.
4. Remove the value of Group2, from unique members, and save the change made.
5. Run `LDAPConfigPostSetup.sh` (on UNIX) or `LDAPConfigPostSetup.bat` (on Windows) to reconcile data from LDAP to Oracle Identity Manager database.

5.2.3.3.5 Description of DomainReassocAuthorization.html Report The report `DomainReassocAuthorization.html` is generated for both 11.1.2 and 11.1.2.1.0 starting points.

It checks if the Oracle Identity Manager domain is reassociated to Database based policy store and displays the result in the **Result** column. Review the checks executed and the result of the checks.

5.2.3.3.6 Description of EVENT_HANDLERPreUpgradeReport.html Report The report `EVENT_HANDLERPreUpgradeReport.html` is generated only for the 11.1.2 starting point.

This report lists all the event handlers that are affected during upgrade. It displays a table with information related to the event handler XML, event handler name, entity type, operation, and stage. The table also contains a **Resolution/Information** column which provides any resolution tasks that need to be completed. Review the information in the table.

5.2.3.3.7 Description of ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html Report The report `ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html` is generated for both 11.1.2 and 11.1.2.1.0 starting points.

This report lists all the mandatory database components or settings for Oracle Identity Manager 11.1.2.x.x upgrade. This report contains a table which lists the component or setting, it's installation or setup status, and recommendations if any. You must review

the installation or setup status for each of the mandatory component or setting listed in the table. If the component or setting is not setup correctly, follow the recommendations specified in the **Note** column of the table in the report to fix them.

5.2.3.3.8 Description of ORACLE_ONLINE_PURGEPreUpgradeReport.html Report Before you upgrade Oracle Identity Manager 11.1.2.x.x to 11.1.2.2.0, you must complete the pre-requisites for online purge.

The table in this report lists the database tables on which the mentioned pre-upgrade steps need to be performed before you upgrade. The table also shows the status of the database tables in **OIM schema** and **Note** section. Review the table, and perform the actions required.

5.2.3.3.9 Description of PasswordPolicyPreUpgradeReport.html Report The report `PasswordPolicyPreUpgradeReport.html` lists the potential upgrade issues for password policies. If you are using 9.1.x.x password policy model, you must update them to new password policies. The 9.1.x.x password policy model is no longer supported for `Users`, and any such customizations done are not migrated to the new password policy model. A default password policy is seeded at `TOP` organization that needs to be revisited.

This report contains a table that lists the password policies that are attached to the `Xellerate User` resource object according to the 9.1.x.x password policy model. You must assign those password policies to appropriate organization(s).

5.2.3.3.10 Description of PROVISIONINGPreUpgradeReport.html Report The report `PROVISIONINGPreUpgradeReport.html` is generated only for 11.1.2.1.0 starting point.

This report lists the potential application instances creation issues. The report contains the following sections:

- Provisioning, Entitlement, and Access Policy Configuration Details
- List of Resource Objects without Process Form
- List of Resource Objects without ITResource field Type in Process Form
- List of Resource Objects with multiple ITResource Lookup fields in Process Form
- List of Access Policies without ITResource value set in default policy data
- List of Access Policies with Revoke If No Longer Applies flag unchecked
- List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value

Provisioning, Entitlement, and Access Policy Configuration Details

This section describes the steps you must complete before you upgrade Oracle Identity Manager 11.1.2.1.0 to 11.1.2.2.0. These steps are related to provisioning, entitlement, and access policy configuration. Complete all the steps described in this section of the report.

List of Resource Objects without Process Form

This section provides information about the resource objects in Oracle Identity Manager 11.1.2.1.0 that do not have process form. Each resource object must have a process form associated with it. Therefore, if a resource object is not associated with a process form, you must associate the resource object with a process form before you start the upgrade process. Review the table in this section of the report, that lists the details of the resource objects without process form.

List of Resource Objects without ITResource field Type in Process Form

This section provides information about the resource objects without ITResource field type in their respective process forms. Review the table in this section of the report, which contains more details. If your Oracle Identity Manager 11.1.2.1.0 has resource objects without ITResource field in their process forms, do the following:

1. Create appropriate IT resource definition.
2. Create IT resource instance for the same corresponding to the target that is being provisioned.
3. Edit the process form and add a field of type "`ITResource`" to the process form. Set the following properties:

   `Type=`*`IT Resource definition created in step-1`*

   `ITResource=true`
4. Activate the form.
5. Update the IT resource field on existing provisioned accounts using FVC Utility.
6. Once the above steps are completed, you can create application instances corresponding to the Resource Object+ITResource combination.

List of Resource Objects with multiple ITResource Lookup fields in Process Form

This section provides information about the resource objects that have multiple lookup fields in their process form. In the Oracle Identity Manager 11.1.2.1.0 environment, if you have resource objects with multiple ITResource set in the process form, you must set the value of the property `ITResource Type` to `true` for at least one of the attributes.

List of Access Policies without ITResource value set in default policy data

This section lists the access policies for which the ITResource values of the resource objects should be set in the default policy data. The table in this section lists the access policies in Oracle Identity Manager 11.1.2.1.0 for which ITResource field is missing. You must set the values of ITResource field for each of the access policy listed in the table.

List of Access Policies with Revoke If No Longer Applies flag unchecked

This section lists the access policies that have `Revoke If No Longer Applies` flag unchecked. The table in this section contains the list of access policies that will be updated to `Disable If No Longer Applies`, during upgrade. The table also indicates if tasks for `enable`, `disable`, `revoke` actions are not defined for these policies. You must add the missing tasks before you proceed with the upgrade. Also, if you want the behavior of the policy to change to RNLA checked, you must check the RNLA flag for the respective policy.

List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value

This section lists entitlements stored in lookup definitions that do not have IT Resource Key pretended to their encoding values using "~". Entitlements stored in lookup definitions need IT Resource Key prepended to the encoded values using "~". Review the table in this section of the pre-upgrade report, which contains more details.

5.2.3.3.11 Description of UDFPreUpgradeReport.html Report

The report `UDFPreUpgradeReport.html` lists the steps that you must complete before you proceed

with the upgrade process, to ensure that the User Defined Fields/Attributes (UDFs) are upgraded seamlessly.

Note that you may have to edit the entity xml file manually. To edit a file in MetaData Services (MDS), you must export the file from MDS repository. After making the required changes, you must import the file back to MDS.

This report contains the following tables:

- Table that lists the path to the entity XML file in MDS corresponding to a particular entity type
- Table that lists the UDFs with inconsistent max-size. You must edit the entity xml file per the list provided in the table, to change the max-size of the attributes to expected values, and re-import the file back into MDS.
- Table that lists the UDFs with inconsistent default values. You must edit the corresponding entity xml file manually to change the default value to one of the allowed values.

5.2.3.3.12 Description of WLSMBEANPreUpgradeReport.html Report The report `WLSMBEANPreUpgradeReport.html` lists the `.jar` files in WebLogic mbeans path that need to be deleted prior to middle tier upgrade. The report contains a table that lists the `.jar` files, their status whether they are present in the WebLogic mbean path, and the action required. Review the information provided in the table, and perform necessary action.

5.2.4 Backing Up Oracle Identity Manager 11.1.2.x.x Environment

You must back up your existing Oracle Identity Manager 11.1.2.x.x environment before you upgrade to Oracle Identity Manager 11.1.2.2.0.

After stopping the servers, back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Identity Manager schema
- MDS schema
- ORASDPM schema
- SOAINFRA schemas
- OPSS schema

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

5.2.5 Setting JVM Properties for Oracle Identity Manager Server(s)

This task is required for optimizing UI performance. Therefore, it is recommended that you set additional JVM properties for the Oracle Identity Manager Server(s) using the WebLogic Administration console. To do this, complete the following steps:

1. Log in to the WebLogic Administration console using the following URL:

   `http://admin_host:admin_port/console`

2. Click **Servers**.

3. Select the Oracle Identity Manager server.
4. Click **Server Start**, and then click **Arguments**.
5. Add the following application module settings for the Oracle Identity Manager Server(s):

```
-Djbo.ampool.doampooling=true
-Djbo.ampool.minavailablesize=1
-Djbo.ampool.maxavailablesize=120
-Djbo.recyclethreshold=60
-Djbo.ampool.timetolive=-1
-Djbo.load.components.lazily=true
-Djbo.doconnectionpooling=true
-Djbo.txn.disconnect_level=1
-Djbo.connectfailover=false
-Djbo.max.cursors=5
-Doracle.jdbc.implicitStatementCacheSize=5
-Doracle.jdbc.maxCachedBufferSize=19
-XX:ReservedCodeCacheSize=128m
```

> **Note:** The recommended values for the argumented specified assume 100 concurrent users per node. Therefore, the value specified for the argument `-Djbo.ampool.maxavailablesize` is `120` (that is, `100 * 1.20`). If the number of concurrent users per node is different, use the following formula to calculate the value that you must specify for the argument `-Djbo.ampool.maxavailablesize`:
>
> `-Djbo.ampool.maxavailablesize = <Number_of_concurrent_users> * 1.20`

6. Restart the Oracle Identity Manager Server(s). To restart Managed Server(s), stop the server(s) first and start them again.

   For more information about stopping a Managed Server, see Section 2.8.1, "Stopping the Managed Server(s)".

   For more information about starting a Managed Server, see Section 2.9.3, "Starting the Managed Server(s)".

5.2.6 Shutting Down Node Manager, Administration Server and Managed Server(s)

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Oracle Identity Manager Managed Server(s), SOA Managed Server(s), WebLogic Administration Server, and the Node Manager.

For information about stopping the WebLogic Administration Server, Managed Server(s), and the Node Manager, see Section 2.8, "Stopping the Servers".

5.3 Upgrading the Oracle Home and Database Schemas

This section describes the tasks to be completed to upgrade the existing Oracle home and Database schemas.

This section includes the following topics:

- Upgrading Oracle WebLogic Server to 10.3.6
- Upgrading Oracle SOA Suite to 11.1.1.7.0
- Upgrading Oracle Identity Manager Binaries to 11.1.2.2.0
- Upgrading Schemas
- Upgrading Oracle Platform Security Services
- Upgrading Java Required Files (JRF)

5.3.1 Upgrading Oracle WebLogic Server to 10.3.6

Oracle Identity and Access Management 11.1.2.2.0 is certified with Oracle WebLogic Server 11*g* Release 1 (10.3.6). Therefore, if your existing Oracle Identity Manager environment is using Oracle WebLogic Server 10.3.5 or the previous versions, you must upgrade Oracle WebLogic Server to 10.3.6.

For information about upgrading Oracle WebLogic Server to 10.3.6, see Section 2.3, "Upgrading to Oracle WebLogic Server 10.3.6".

5.3.2 Upgrading Oracle SOA Suite to 11.1.1.7.0

Oracle Identity Manager 11.1.2.2.0 is certified with Oracle SOA Suite 11g Release 1 (11.1.1.7.0). If you are not using Oracle SOA Suite 11.1.1.7.0, you must upgrade your existing Oracle SOA Suite to 11.1.1.7.0 by completing the tasks listed in Table 5–7.

Table 5–7 Tasks to Upgrade SOA to 11.1.1.7.0

Sl No	Task	For More Information
1	Review the system requirements and specifications before you start upgrading Oracle SOA Suite to 11.1.1.7.0.	See, Oracle Fusion Middleware System Requirements and Specifications
2	Obtain the Oracle SOA Suite 11.1.1.7.0 installer.	See, *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*
3	Start the Oracle SOA Suite 11.1.1.7.0 installer.	See, "Start the Installer" in the *Oracle Fusion Middleware Patching Guide*
4	Update the Oracle SOA Suite binaries to 11.1.1.7.0.	See, "Applying the Patch Set" in the *Oracle Fusion Middleware Patching Guide*
5	Apply the mandatory Oracle SOA Suite patches.	See, "Mandatory Patches Required for Installing Oracle Identity Manager" in the *Oracle Fusion Middleware Release Notes*.

Table 5–7 (Cont.) Tasks to Upgrade SOA to 11.1.1.7.0

Sl No	Task	For More Information
6	Perform the following post-patching tasks for Oracle SOA Suite: ■ Remove the tmp folder for SOA composer, BPM workspace, and B2B. ■ Update the message duration of the warning `BPEL Message Recovery Required`. ■ Update the `MAXRECOVERATTEMPT` attribute to `2`. ■ Extend the SOA domain with UMS adapter features. ■ Extend the SOA domain with Business Process Management features. Make sure you have started the WebLogic Administration Server and the SOA Managed Servers before you perform the post-patching tasks.	See the following sections in the *Oracle Fusion Middleware Patching Guide* for 11*g* Release 1 (11.1.1.7.0): ■ Removing the tmp Folder for SOA Composer, BPM Workspace and B2B ■ Updating the "BPEL Message Recovery Required" Warning Message Duration ■ Updating MAXRECOVERATTEMPT Attribute to 2 ■ Extending the SOA Domain with UMS Adapter Features ■ Extending the SOA Domain with Business Process Management Features Post-patching tasks for SOA are not required out-of-the-box. However, you must review them and apply per your functional requirements.

5.3.3 Upgrading Oracle Identity Manager Binaries to 11.1.2.2.0

You must upgrade the Oracle Identity Manager 11.1.2.x.x binaries Oracle Identity Manager 11.1.2.2.0 using the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Installer. During the procedure, point the Middleware Home to your existing 11.1.2.x.x Middleware Home. This upgrades the Oracle Identity Manager binaries 11.1.2.2.0.

Note: Before upgrading the Oracle Identity Manager binaries to 11*g* Release 2 (11.1.2.2.0), you must ensure that the OPatch version in *ORACLE_HOME* and *MW_HOME*/oracle_common is 11.1.0.9.9. Different OPatch version might cause patch application failure. If you have upgraded opatch to a newer version, you will have to roll back to version 11.1.0.9.9.

For information about updating Oracle Identity Manager binaries to 11.1.2.2.0, see Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0).

After the binary upgrade, check the installer logs at the following location:

- On UNIX: *ORACLE_INVENTORY_LOCATION*/logs

  To find the location of the Oracle Inventory directory on UNIX, check the file *ORACLE_HOME*/oraInst.loc.

- On Windows: *ORACLE_INVENTORY_LOCATION*\logs

  The default location of the Oracle Inventory Directory on Windows is `C:\Program Files\Oracle\Inventory\logs`.

The following install log files are written to the log directory:

- install*DATE-TIME_STAMP*.log

- install*DATE-TIME_STAMP*.out
- installActions*DATE-TIME_STAMP*.log
- installProfile*DATE-TIME_STAMP*.log
- oraInstall*DATE-TIME_STAMP*.err
- oraInstall*DATE-TIME_STAMP*.log

5.3.4 Upgrading Schemas

After you update Oracle Identity Manager binaries to 11.1.2.2.0, you must upgrade the following schemas using Patch Set Assistant (PSA):

- OPSS schema
- MDS schema
- OIM schema
- ORASDPM schema
- SOAINFRA schema

When you select the Oracle Identity Manager Schema, it automatically selects all dependent schemas and upgrades them too.

For information about upgrading schemas using the Patch Set Assistant, see Upgrading Schemas Using Patch Set Assistant.

After you upgrade schemas, verify the upgrade by checking the version numbers of the schemas as described in Version Numbers After Upgrading Schemas.

Version Numbers After Upgrading Schemas

Connect to oim schema as *oim_schema_user*, and run the following query:

```
select version,status,upgraded from schema_version_registry where
owner=<SCHEMA_NAME>;
```

Ensure that the version numbers are upgraded, as listed in Table 5–8:

Table 5–8 Component Version Numbers After Upgrading the Schemas

Component	Version No.
OPSS	11.1.1.7.2
MDS	11.1.1.7.0
OIM	11.1.2.2.0
ORASDPM	11.1.1.7.0
SOAINFRA	11.1.1.7.0

5.3.5 Upgrading Oracle Platform Security Services

After you upgrade schemas, you must upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Identity Manager to 11.1.2.2.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see Section 2.7, "Upgrading Oracle Platform Security Services".

5.3.6 Upgrading Java Required Files (JRF)

For each WebLogic Server domain, you must run the `upgradeJRF()` WLST command to update the shared libraries in your domain. To do this, complete the following steps:

1. Stop all running instances, Managed Servers, Administration Server, and Node Manager in the domain. For information about stopping the servers, see Section 2.8, "Stopping the Servers".
2. Launch WebLogic Scripting Tool (WLST) by running the following commands:

   On UNIX:

   ```
   cd MW_HOME/oracle_common/common/bin

   ./wlst.sh
   ```

   On Windows:

   ```
   cd MW_HOME\oracle_common\common\bin

   wlst.cmd
   ```

3. Run the `upgradeJRF()` command on the node or system where the Administration Server is located for each domain you want to update. Your domain location is passed as a parameter:

   ```
   wlst> upgradeJRF('DOMAIN_HOME')
   ```

   In this command, *DOMAIN_HOME* refers to the absolute path to the domain.

   Note: After you run this command, any custom changes that you have made to your `setDomainEnv` script will be lost. Oracle recommends that you keep your custom modifications in a separate script that is called by `setDomainEnv` in order to minimize the disruption that is caused when other domain templates are applied and the `setDomainEnv` script is regenerated.

   If you have set IPv6 to false in your `setDomainEnv` script, this change will be overwritten when you run the `upgradeJRF()` command. Make sure you reset IPv6 to `false` in the `setDomainEnv` script after you run the `upgradeJRF()` command.

5.4 Upgrading the Oracle Identity Manager Middle Tier

This section describes the tasks to be completed to upgrade the Oracle Identity Manager middle tier.

This section includes the following topics:

- Starting Administration Server and SOA Managed Server(s)
- Upgrading Oracle Identity Manager Middle Tier
- Restarting all the Servers

5.4.1 Starting Administration Server and SOA Managed Server(s)

After the binary and schema upgrade are completed, start the WebLogic Administration Server, and SOA Managed Server.

> **Note:** If you are upgrading Oracle Identity Manager high availability environments and if you are using Oracle Automatic Storage Management Cluster File System (Oracle ACFS), you must start only one SOA Managed Server before running the middle tier upgrade utility.

For information about starting the WebLogic Administration Server and the Managed Server(s), see Section 2.9, "Starting the Servers".

5.4.2 Upgrading Oracle Identity Manager Middle Tier

This section contains the following topics:

- Additional Task for Windows 64-Bit Users Before Upgrading Middle Tier
- Upgrading the Oracle Identity Manager Middle Tier
- Verifying the Middle Tier Upgrade

5.4.2.1 Additional Task for Windows 64-Bit Users Before Upgrading Middle Tier

If you are running the upgrade in a 64-bit Windows platform, complete the following task to run Middle Tier upgrade successfully:

1. Add a *JAVA_HOME* entry to the environment variable pointing to a JDK installation, not to a JRE installation.

   > **Note:** This path should be without spaces or like `C:\Progra~1\Java\jdk1.6.0_29`.

2. Hard code the value of *JAVA_HOME* in `<WL_HOME>\server\bin\setWLSEnv.cmd` file to avoid any Middle Tier upgrade failures.

5.4.2.2 Upgrading the Oracle Identity Manager Middle Tier

To upgrade the Oracle Identity Manager middle tier, you must update the properties file with the necessary parameters, and then run the command as described in this section.

> **Note:** Before you upgrade the Oracle Identity Manager middle tier, make sure that the WebLogic Administration Server and the SOA Managed Server(s) are running. It is recommended that the Oracle Identity Manager Managed Server is not running at this point.

> **Note:** The execution is re-entrant and will resume with correct execution even if there is any interruption in between.

To upgrade Oracle Identity Manager Middle Tier to 11.1.2.2.0, do the following:

On UNIX:

1. Move from your present working directory to the *OIM_ORACLE_HOME*/server/bin directory by running the following command on the command line:

   ```
   cd OIM_ORACLE_HOME/server/bin
   ```

2. Edit the following upgrade properties file in a text editor:

   ```
   oim_upgrade_input.properties
   ```

3. Provide the values of parameters as listed in Table 5–9.

4. Run the following command:

   ```
   ./OIMUpgrade.sh
   ```

   Note: The following warning is displayed:

   ```
   [WARN ][jrockit] PermSize=128M ignored: Not a valid option
   for JRockit

   [WARN ][jrockit] MaxPermSize=256M ignored: Not a valid
   option for JRockit
   ```

   You can ignore this message.

On Windows:

1. Move from your present working directory to the *OIM_ORACLE_HOME*\server\bin directory by running the following command on the command line:

   ```
   cd OIM_ORACLE_HOME\server\bin
   ```

2. Edit the following upgrade properties file in a text editor:

   ```
   oim_upgrade_input.properties
   ```

3. Provide the values of parameters as listed in Table 5–9.

4. Run the following command:

   ```
   OIMUpgrade.bat
   ```

   Note: The following warning is displayed:

   ```
   [WARN ][jrockit] PermSize=128M ignored: Not a valid option
   for JRockit

   [WARN ][jrockit] MaxPermSize=256M ignored: Not a valid
   option for JRockit
   ```

   You can ignore this message.

Table 5–9 Parameters to be specified in the Properties File

Parameter	Description
`java.home`	Specify the JAVA HOME location.

Table 5–9 (Cont.) Parameters to be specified in the Properties File

Parameter	Description
server.type	Specify the Application Server that you are using. For example, if you are using Oracle WebLogic Server, specify wls for this parameter; or if you are using IBM WebSphere, specify was. As this document describes the procedure to upgrade Oracle Identity Manager on WebLogic, you must specify wls for this parameter.
oim.jdbcurl	Specify the Oracle Identity Manager JDBC URL.
oim.oimschemaowner	Specify the Oracle Identity Manager schema owner.
oim.oimmdsjdbcurl	Specify the MDS JDBC URL.
oim.mdsschemaowner	Specify the MDS schema owner name.
oim.adminhostname	Specify the Oracle WebLogic Server Administration host name.
oim.adminport	Specify the Oracle WebLogic Server Administration port.
oim.adminUserName	Specify the username that is used to log in to the Oracle WebLogic Server Administration Console.
oim.soahostmachine	Specify the SOA host name where SOA Server is running.
oim.soaportnumber	Specify the SOA Server port.
oim.soausername	Specify the SOA Managed Server username.
oim.domain	Specify the Oracle Identity Manager domain location.
oim.home	Specify the Oracle OIM Home location.
oim.mw.home	Specify the Oracle Middleware Home location.
soa.home	Specify the Oracle SOA Home location.
wl.home	Specify the WebLogic Home location.

Example Parameters:

```
java.home=/scratch/jdk1.7.0_11
server.type=wls
oim.jdbcurl=db.example.com:1522:oimdb
oim.oimschemaowner=dev_oim
oim.oimmdsjdbcurl=db.example.com:1521:oimdb
oim.mdsschemaowner=dev_mds
oim.adminhostname=oimhost.example.com
oim.adminport=7001
oim.adminUserName=weblogic
oim.soahostmachine=soahost.example.com
oim.soaportnumber=8001
oim.soausername=weblogic
oim.domain=/scratch/Oracle/Middleware/user_projects/domains/base_domain
oim.home=/scratch/Oracle/Middleware/Oracle_IDM1
oim.mw.home=/scratch/Oracle/Middleware
soa.home=/scratch/Oracle/Middleware/Oracle_SOA1
wl.home=/scratch/Oracle/Middleware/wlserver_10.3
```

5.4.2.3 Verifying the Middle Tier Upgrade

Middle tier upgrade utility creates log file and HTML reports with upgrade details for feature. To verify that the Oracle Identity Manager middle tier upgrade was successful, do the following:

After the Oracle Identity Manager middle tier upgrade, verify the log file `ant_grantPermissionsUpgrade.log` generated at the location *`OIM_HOME`*`/server/upgrade/logs/MT` to ensure that the middle tier upgrade was successful.

1. Verify the log file `ant_grantPermissionsUpgrade.log` generated at the location *`OIM_HOME`*`/server/upgrade/logs/MT` to ensure that the middle tier upgrade was successful.
2. Review the HTML upgrade reports generated at the location *`MW_HOME`*`/`*`OIM_HOME`*`/server/upgrade/logs/MT/oimUpgradeReportDir`. The `index.html` report in this directory lists all the features upgraded during the middle tier upgrade.

5.4.3 Restarting all the Servers

After you upgrade the Oracle Identity Manager middle tier, you must restart the WebLogic Administration Server, Oracle Identity Manager Managed Server, and the SOA Managed Server.

To restart the servers, you must stop the servers first and start them again in the following order:

1. Stop the SOA Managed Server.
2. Stop the WebLogic Administration Server.
3. Start the WebLogic Administration Server.
4. Start the SOA Managed Server.
5. Start the Oracle Identity Manager Managed Server.

For more information about stopping the servers, see Section 2.8, "Stopping the Servers".

For more information about starting the servers, see Section 2.9, "Starting the Servers".

5.5 Upgrading Other Oracle Identity Manager Installed Components

This section describes how to upgrade other Oracle Identity Manager installed components such as Oracle Identity Manager Design Console and Remote Manager to 11.1.2.2.0.

This section includes the following sections:

- Upgrading Oracle Identity Manager Design Console
- Upgrading Oracle Identity Manager Remote Manager

5.5.1 Upgrading Oracle Identity Manager Design Console

The Oracle Identity Manager Design Console is used to configure system settings that control the system-wide behavior of Oracle Identity Manager and affect its users. The Design Console allows you to perform user management, resource management, process management, and other administration and development tasks.

Oracle recommends that Oracle Identity Manager and Design Console are installed in different directory paths, if the Design console is on the same system as the Oracle Identity Manager server.

To upgrade Design Console, complete the following steps:

1. Back up the following files:
   - On UNIX, `$<XLDC_HOME>/xlclient.sh`
   - `$<XLDC_HOME>/config/xlconfig.xml`
   - On Windows, `<XLDC_HOME>\xlclient.cmd`
   - `<XLDC_HOME>\config\xlconfig.xml`
2. Run the Oracle Identity and Access Management 11.1.2.2.0 Installer to upgrade the Design Console home `<XLDC_HOME>`.

   For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2.2.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
3. Restore the following backed up files in the upgraded Design Console home:

   On UNIX:
   - `xlclient.sh`
   - `xlconfig.xml`

   On Windows:
   - `xlclient.cmd`
   - `xlconfig.xml`
4. Build and copy the `wlfullclient.jar` file as follows:
   a. Go to `WebLogic_Home/server/lib` directory on UNIX and `WebLogic_Home\server\lib` directory on Windows.
   b. Set the `JAVA_HOME` environment variable and add the `JAVA_HOME` variable to the `PATH` environment variable. You can set the `JAVA_HOME` to the `jdk160_21` directory inside the Middleware home.

      For example:

      On UNIX: `setenv JAVA_HOME $MW_HOME/jdk160_29`

      On Windows: `SET JAVA_HOME="MW_HOME\jdk160_29"`
   c. Run the following command to build the `wlfullclient.jar` file:

      ```
      java -jar <MW_HOME>/modules/com.bea.core.jarbuilder_1.7.0.0.jar
      ```
   d. Copy the `wlfullclient.jar` file to the `<IAM_HOME>` where you installed the Design Console. For example:

      On UNIX:

      ```
      cp wlfullclient.jar <Oracle_IDM2>/designconsole/ext
      ```

      On Windows:

      ```
      copy wlfullclient.jar <Oracle_IDM2>\designconsole\ext
      ```

5.5.2 Upgrading Oracle Identity Manager Remote Manager

Complete the following steps to upgrade Remote Manager:

1. Back up configuration files

   Before starting the Remote Manager upgrade, back up the following Remote Manager configuration files:

   - On UNIX, `$<XLREMOTE_HOME>/remotemanager.sh`
   - `$<XLREMOTE_HOME>/xlremote/config/xlconfig.xml` file.
   - On Windows, `<XLREMOTE_HOME>\remotemanager.bat`
   - `<XLREMOTE_HOME>\xlremote\config\xlconfig.xml` file.

2. Run the Oracle Identity and Access Management Installer to upgrade the Remote Manager home.

   For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2.2.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

3. Restore the following backed up configuration files in the upgraded Remote Manager home.

   On UNIX:

   - `remotemanager.sh`
   - `xlconfig.xml`

   On Windows:

   - `remotemanager.bat`
   - `xlconfig.xml`

5.6 Post-Upgrade Steps

This section describes the post-upgrade tasks that you must perform after you upgrade Oracle Identity Manager 11.1.2.x.x to Oracle Identity Manager 11.1.2.2.0.

This section includes the following topics:

- Performing the Post-Upgrade Tasks
- Verifying the Upgrade

5.6.1 Performing the Post-Upgrade Tasks

After you upgrade Oracle Identity Manager 11.1.2.x.x to 11.1.2.2.0, you must perform the following mandatory post-upgrade tasks

- Reviewing Performance Tuning Recommendations
- Upgrading Request Data
- Configuring BI Publisher Reports
- Targeting JRFWSAsyncJmsModule to Oracle Identity Manager Server
- Creating PeopleSoft Enterprise HRMS Reconciliation Profile
- Reviewing OIM Data Purge Job Parameters
- Reconfiguring Lookup Based UDF Field

- Reviewing Connector Certification
- Verifying the Functionality of Connectors

5.6.1.1 Reviewing Performance Tuning Recommendations

After you upgrade to Oracle Identity Manager 11.1.2.2.0, you must review the Oracle Identity Manager specific performance tuning recommendations described in "Oracle Identity Manager Performance Tuning" in the *Oracle Fusion Middleware Performance and Tuning Guide*.

5.6.1.2 Upgrading Request Data

You must upgrade the request data by running the request data upgrade utility. This utility updates Metadata Services (MDS) and the request tables. To upgrade the request data, do the following:

1. Set the environment variables `MW_HOME`, `ORACLE_HOME`, `ANT_HOME`, and `JAVA_HOME` by running the following commands:

   On UNIX:

   - `export ORACLE_HOME=<absolute_path_to_OIM_home>`
   - `export MW_HOME=<absolute_path_to_Middleware_home>`
   - `export ANT_HOME=<absolute_path_to_directory_where_you_uncompressed_Ant>`
   - `export JAVA_HOME=<absolute_path_to_jdk_location>`

   On Windows:

   - `set OIM_HOME="<absolute_path_to_OIM_home>"`
   - `set MW_HOME="<absolute_path_to_Middleware_home>"`
   - `set ANT_HOME="<absolute_path_to_directory_where_you_uncompressed_Ant>`
   - `set JAVA_HOME="<absolute_path_to_jdk_location>"`

2. Edit the file `run-request-automation.xml` at the location *ORACLE_HOME*`/server/bin`, and provide the Database details for OIM and MDS schemas in the arguments tag by replacing the existing values.

   For example:

```
<arg value="dev_oim"/>
<arg value="${dbpassword}"/>
<arg value="dev_mds"/>
<arg value="${mdspassword}"/>
<arg value="oim.db.example.com"/>
<arg value="1521"/>
<arg value="oim.db.servicename.example.com"/>
<arg value="mds.db.example.com"/>
<arg value="1521"/>
<arg value="mds.db. servicename.example.com "/>
```

Note: Leave the OIM and MDS passwords as is. The utility will prompt for passwords.

3. Run the `run-request-automation.xml` file using the following command:

   ```
   ant -f run-request-automation.xml
   ```

4. Verify the logs at the location *$ORACLE_HOME*`/server/patching/logs` to ensure that the request data upgrade was successful.

5. Run the PurgeCache utility from the location *OIM_HOME*`/server/bin` with category `MetaData` using the following command:

   On UNIX: `PurgeCache.sh Metadata`

   On Windows: `PurgeCache.bat Metadata`

5.6.1.3 Configuring BI Publisher Reports

Complete the following steps to configure the BI Publisher Reports:

1. Obtain the reports bundle `oim_product_BIP11gReports_11_1_2_1_0.zip` from the following location:

   OIM_HOME`/server/reports/oim_product_BIP11gReports_11_1_2_1_0.zip`

2. Unzip `oim_product_BIP11gReports_11_1_2_1_0.zip` at the following location:

   MW_HOME`/user_projects/domains/domain_name/config/bipublisher/repository/Reports/`

3. Configure reports by following the instructions in "Configuring Oracle Identity Manager Reports" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

5.6.1.4 Targeting JRFWSAsyncJmsModule to Oracle Identity Manager Server

If you wish to use async webservices for SoD integration, you must target the `JRFWSAsyncJmsModule` to the Oracle Identity Manager Server.

Perform this task in the following cases:

- If you are upgrading Oracle Identity Manager 11.1.2 to 11.1.2.2.0
- If you upgraded Oracle Identity Manager 11.1.2 to 11.1.2.1.0 first and then to 11.1.2.2.0; and if you did not target `JRFWSAsyncJmsModule` to Oracle Identity Manager Server when upgrading Oracle Identity Manager 11.1.2 to 11.1.2.1.0.

To target `JRFWSAsyncJmsModule` to the Oracle Identity Manager server, do the following:

1. Log in to the WebLogic Administration console using the following URL:

   `http://`*admin_host*`:`*admin_port*`/console`

2. Click **Services** and then click **Messaging**.

3. Select **JMS Modules**.

4. Select **JRFWSAsyncJmsModule**.

5. Select **Targets**, and add the OIM Server.

6. Save and Activate the changes.

7. Restart the WebLogic Administration Server, the SOA Managed Server(s), and the Oracle Identity Manager Managed Server(s) by completing the following steps in the order specified:

   1. Stop the SOA Managed Server(s).

2. Stop the WebLogic Administration Server.
3. Start the WebLogic Administration Server.
4. Start the SOA Managed Server(s).
5. Start the Oracle Identity Manager Managed Server(s).

For more information about stopping the servers, see Section 2.8, "Stopping the Servers".

For more information about starting the servers, see Section 2.9, "Starting the Servers".

5.6.1.5 Creating PeopleSoft Enterprise HRMS Reconciliation Profile

If you are upgrading Oracle Identity Manager 11.1.2 with PeopleSoft connector to Oracle Identity Manager 11.1.2.2.0, you must create PeopleSoft HRMS reconciliation profile after you upgrade to 11.1.2.2.0. For information about creating reconciliation profile, see "Updating Reconciliation Profiles Manually" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

5.6.1.6 Reviewing OIM Data Purge Job Parameters

This post-upgrade task is optional.

While upgrading Oracle Identity Manager to 11.1.2.2.0, the `OIM Data Purge Job` will be seeded in `enabled` state. By default, it will purge platform data with a retention period of 1 day for completed orchestration. To enable purge of request, reconciliation, and provisioning task, you must revisit the `OIM Data Purge Job` parameters.

For information about the user-configurable attributes, see "Configuring Real-Time Purge and Archival" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

5.6.1.7 Reconfiguring Lookup Based UDF Field

If you had User Defined Fields (UDF) of type lookup or dropdown as **outputText** field in your 11.1.2.x.x environment, you will see backend value for that UDF on the **View User Details** page. Therefore, you must complete the following steps to set the right customizations:

1. Log in to the Identity console using the following URL:

   `http://host:port/identity`

2. Click **Sandboxes** on the top naviagtion pane, and then click **Create Sandbox**.
3. Enter the **Sandbox Name** and the **Sandbox Description**. Select the check box **Activate Sandbox**, and then click **Save and Close**. Click **OK** to confirm.
4. Click **Customize** on the top navigation pane.
5. Click **Users** on the left navigation pane, and select the user to open the **User Details** page.
6. Click **View** on the top left cornor of the console, and select **Source**.
7. Select the existing **outputText** field. Click **Delete** to delete this field.
8. Close the customize mode, and publish the sandbox by clicking **Publish Sandbox**.
9. Export the metadata file `userDetailsPageDef.xml` to MDS. The following is the full path to the file to be exported:

`/oracle/iam/ui/manageusers/pages/mdssys/cust/site/site/userDetailsPageDef.xml`

For information about exporting metadata files to MDS, see "Exporting Metadata Files to MDS" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

10. Open the exported file in a text editor.
11. Search for the dropdown or lookup attribute that was added as **outputText**. For example, if the attribute name is `lovattr`, search for a snippet similar to the following:

```
<mds:insert parent="..." position="...">
 <attributeValues IterBinding="..." id="lovattr__c" xmlns="...">
  <AttrNames>
   <Item Value="lovattr__c"/>
  </AttrNames>
 </attributeValues>
</mds:insert>
```

Delete the snippet, that is, delete the lines starting from the `<mds:insert .... >` tag till the `</mds:insert>` tag.

Repeat this step for all dropdown or lookup attributes.

12. Save the file.
13. Import the `userDetailsPageDef.xml` back into the MDS. For information about importing metadata file, see "Importing Metadata Files from MDS" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
14. Log in to the Identity console again.
15. Create another sandbox by clicking **Create Sandbox**. Enter the **Sandbox Name** and the **Sandbox Description**. Select the check box **Activate Sandbox**, and then click **Save and Close**. Click **OK** to confirm.
16. Click **Customize** on the top navigation pane.
17. Click **Users** on the left navigation pane, and select the user to open the **User Details** page.
18. Click **View** on the top left corner of the console, and select **Source**.
19. Add the LOV dropdown field as **ADF Select one choice (if NON searchable) ' , 'Input list of values (If Searchable picklist)'** to the required section.
20. Select **readonly** on the **Component Properties dialog** box.
21. Close the customize mode, and publish the sandbox by clicking **Publish Sandbox**.

5.6.1.8 Reviewing Connector Certification

Before you upgrade your existing Oracle Identity Manager environments, you must verify if the version of the existing connector is supported for Oracle Identity Manager 11.1.2.2.0. For information about the supported connector versions for Oracle Identity Manager 11.1.2.2.0, refer to the sections "Certified Components" and "Usage Recommendation" in the respective *Connector Guide* in Oracle Identity Manager Identity Connectors Documentation Library.

If you are using 9.x connector or GTC connector, do the following:

- If the 9.x connector that you are using is supported, you can continue to use the existing connector.

- If the 9.x connector is not supported, you must upgrade the existing 9.x connector to the latest 11.x connector after you upgrade the Oracle Identity Manager server to 11.1.2.2.0.
- Verify the data in the `Lookup` populated through lookup reconciliation that the IT Resource Key & IT Resource name is pre-fixed for code & decode respectively. If not, you must upgrade the existing connector to the latest available connector after you upgrade Oracle Identity Manager server.

If you are using 11g connector, the connector upgrade is not required.

5.6.1.9 Verifying the Functionality of Connectors

After you upgrade Oracle Identity Manager to 11.1.2.2.0, complete the following steps to verify the functionality of connectors:

- Verify if Account and Entitlement Tagging are available on the process form. For the connectors to work with Oracle Identity Manager 11.1.2.2.0, you must complete the steps described in the section "Configuring Oracle Identity Manager 11.1.2 or Later" in the respective *Connector Guide*.
- Verify if the customizations made to the connectors are intact.
- Verify if the 11.1.2.2.0 related artifacts like UI Forms and Application Instances are generated.
- Ensure that all the operations of the connectors are working fine.
- If there are two or more IT Resource field in the process form, complete the steps described in the following My Oracle Support note:

  My Oracle Support document ID 1535369.1
- If there are any lookup query fields in the process form of the related connector, then you must customize the UI need to display the same. For more information, see 'Lookup Query' section in "General Customization Concepts" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

5.6.2 Verifying the Upgrade

To verify your Oracle Identity Manager upgrade, perform the following steps:

1. Use the following URL in a web browser to verify that Oracle Identity Manager 11.1.2.2.0 is running:

   `http://<oim_host>:<oim_port>/sysadmin`

   `http://<oim_host>:<oim_port>/identity`

   where

   <oim_host> is the domain name.

   <oim_port> is the port number.
2. Use Fusion Middleware Control to verify that Oracle Identity Manager and any other Oracle Identity Management components are running in the Oracle Fusion Middleware environment.

Note: SOA composites `DefautlRequestApproval` and `DefaultOperationApproval` are available twice with versions `1.0` and `3.0` on Oracle Enterprise Manager, after you upgrade Oracle Identity Manager 11.1.2 or 11.1.2.1.0 to Oracle Identity Manager 11.1.2.2.0. The `1.0` composites are required for processing requests generated before upgrade, or any other functionality.

6

Upgrading Oracle Entitlements Server 11*g* Release 2 (11.1.2.x.x) Environments

This chapter describes how to upgrade Oracle Entitlements Server 11*g* Release 2 (11.1.2.1.0) and 11*g* Release 2 (11.1.2) environments to Oracle Entitlements Server 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

Note: For information about upgrading Oracle Entitlements Server on IBM WebSphere, see "Upgrading Oracle Entitlements Server 11g Release 2 (11.1.2.1) to 11g Release 2 (11.1.2.2.0)" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

Note: This chapter refers to Oracle Entitlements Server 11*g* Release 2 (11.1.2) and 11*g* Release 2 (11.1.2.1.0) environments as 11.1.2.x.x.

This chapter includes the following sections:

- Upgrading Oracle Entitlements Server 11.1.2.x.x Administration Server
- Upgrading Oracle Entitlements Server 11.1.2.x.x Client

6.1 Upgrading Oracle Entitlements Server 11.1.2.x.x Administration Server

This section describes how to upgrade Oracle Entitlements Server Administration Server to 11.1.2.2.0.

This section includes the following topics:

- Section 6.1.1, "Upgrade Roadmap for Oracle Entitlements Server Administration Server"
- Section 6.1.2, "Reviewing System Requirements and Certification"
- Section 6.1.3, "Shutting Down Administration Server and Oracle Entitlements Server Managed Servers"
- Section 6.1.4, "Upgrading Oracle WebLogic Server (If Necessary)"
- Section 6.1.5, "Updating Oracle Entitlements Server Binaries to 11.1.2.2.0"
- Section 6.1.6, "Upgrading Oracle Platform Security Services Schema"
- Section 6.1.7, "Upgrading Oracle Platform Security Services"

- Section 6.1.8, "Deleting Certain Directories From the Domain"
- Section 6.1.9, "Starting the Administration Server and the Managed Servers"
- Section 6.1.10, "Verifying the Oracle Entitlements Server Administration Server Upgrade"

6.1.1 Upgrade Roadmap for Oracle Entitlements Server Administration Server

Table 6–1 lists the steps to upgrade Oracle Entitlements Server Administration Server upgrade.

Note: If you do not follow the exact sequence provided in this task table, your Oracle Entitlements Server Administration Server upgrade may not be successful.

Table 6–1 Roadmap for Upgrading Oracle Entitlements Server Administration Server 11.1.2.x.x to 11.1.2.2.0

Sl No	Task	For More Information
1	Review system requirements and certifications.	See, Reviewing System Requirements and Certification
2	Stop the Administration Server and all the Oracle Entitlements Server Managed Servers.	See, Shutting Down Administration Server and Oracle Entitlements Server Managed Servers
3	Upgrade your existing Oracle WebLogic Server to 10.3.6 (if necessary).	See, Upgrading Oracle WebLogic Server (If Necessary)
4	Upgrade the Oracle Entitlements Server binaries to 11.1.2.2.0.	See, Updating Oracle Entitlements Server Binaries to 11.1.2.2.0
5	Upgrade the Oracle Platform Security Services schemas.	See, Upgrading Oracle Platform Security Services Schema
6	Upgrade Oracle Platform Security Services to 11.1.2.2.0. This task is optional but is recommended.	See, Upgrading Oracle Platform Security Services
7	Delete the `tmp`, `cache`, and `stage` directories from the domain.	See, Deleting Certain Directories From the Domain
8	Start all the servers.	See, Starting the Administration Server and the Managed Servers
9	Verify the Oracle Entitlements Server Administration Server upgrade.	See, Verifying the Oracle Entitlements Server Administration Server Upgrade

6.1.2 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see Section 2.1, "Reviewing System Requirements and Certification".

6.1.3 Shutting Down Administration Server and Oracle Entitlements Server Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Oracle Entitlements Server Managed Server(s) and the WebLogic Administration Server.

For information about stopping the WebLogic Administration Server and the Managed Servers, see Section 2.8, "Stopping the Servers".

6.1.4 Upgrading Oracle WebLogic Server (If Necessary)

Note: Upgrading Oracle WebLogic Server is not mandatory. However, Oracle recommends that you upgrade Oracle WebLogic Server to 10.3.6.

If you are not using Oracle WebLogic Server 10.3.6, you can upgrade your existing WebLogic Server to 10.3.6 by using the WebLogic 10.3.6 Upgrade Installer. Complete the following steps:

For information about upgrading to Oracle WebLogic Server 10.3.6, see Section 2.3, "Upgrading to Oracle WebLogic Server 10.3.6".

6.1.5 Updating Oracle Entitlements Server Binaries to 11.1.2.2.0

To upgrade Oracle Entitlements Server binaries to 11.1.2.2.0, you must use the Oracle Identity and Access Management 11.1.2.2.0 Installer. During the procedure, point the Middleware Home to your existing 11.1.2.x.x Middleware Home.

For information about updating the Oracle Entitlements Server binaries to 11.1.2.2.0, see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

6.1.6 Upgrading Oracle Platform Security Services Schema

After updating the Oracle Entitlements Server binaries, you must upgrade the Oracle Platform Security Services schemas using Patch Set Assistant. To do this, complete the following steps:

1. Start the Patch Set Assistant from the location *MW_HOME*`/oracle_common/bin` using the following command:

   ```
   ./psa
   ```

2. Select **opss**.

3. Specify the Database connection details, and select the schema to be upgraded.

After you upgrade Oracle Platform Security Services schema, verify the upgrade by checking the log file at the location *MW_HOME*`/oracle_common/upgrade/logs/psa<`*timestamp*`>.log`.

The *timestamp* refers to the actual date and time when Patch Set Assistant was run. If the upgrade fails, check the log files to rectify the errors and run the Patch Set Assistant again.

For more information about upgrading schemas using Patch Set Assistant, see Section 2.6, "Upgrading Schemas Using Patch Set Assistant".

6.1.7 Upgrading Oracle Platform Security Services

After you upgrade Oracle Platform Security Services schemas, you must upgrade Oracle Platform Security Services (OPSS). This task is optional; however, it is recommended that you perform this task.

> **Note:** If you are upgrading Oracle Entitlements Server 11.1.2.1.0 to 11.1.2.2.0, you must upgrade Oracle Platform Security Services if Audit schema is installed. This step is required to upgrade the policy store to include the new 11.1.2.2.0 audit policies.

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Entitlements Server to 11.1.2.2.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see Section 2.7, "Upgrading Oracle Platform Security Services".

6.1.8 Deleting Certain Directories From the Domain

Delete the following directories from the location *DOMAIN_HOME*`/servers/`*ServerName*:

- `tmp`
- `cache`
- `stage`

6.1.9 Starting the Administration Server and the Managed Servers

After the upgrade is complete, start the WebLogic Administration Server, and the Oracle Entitlements Server Managed Server(s).

For information about starting the WebLogic Administration Server and the Managed Server(s), see Section 2.9, "Starting the Servers".

6.1.10 Verifying the Oracle Entitlements Server Administration Server Upgrade

To verify the Oracle Entitlements Server upgrade, do the following:

- Verify the schema version in the policy store by running the following SQL query:

  ```
  select attrval from jps_attrs where attrname='orclProductVersion' and
  rownum = 1;
  ```

  Ensure that the schema version is 11.1.1.7.2.

- The application MAPI works with both old and new functionalities.

  Create a new policy to see if CRUD operations on the policy store artifacts, using their entity managers, are working.

  For more information, see "Creating Fine Grained Elements for a Simple Policy" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*.

- The Application Runtime Authorization continues working.

  To verify, create an authorization, as mentioned in "Using the PEP API" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*, and see if it works correctly.

6.2 Upgrading Oracle Entitlements Server 11.1.2.x.x Client

This section descries how to upgrade Oracle Entitlements Server client server to 11.1.2.2.0.

This section includes the following topics:

- Section 6.2.1, "Upgrade Roadmap for Oracle Entitlements Server Client"
- Section 6.2.2, "Stopping all Security Module Instances"
- Section 6.2.3, "Upgrade Oracle Entitlements Server Client to 11.1.2.2.0"
- Section 6.2.4, "Starting the Security Modules"
- Section 6.2.5, "Verifying Oracle Entitlements Server Client Upgrade"

6.2.1 Upgrade Roadmap for Oracle Entitlements Server Client

Table 6–2 lists the steps to upgrade Oracle Entitlements Server Client Server upgrade.

Note: If you do not follow the exact sequence provided in this task table, your Oracle Entitlements Server Client Server upgrade may not be successful.

Table 6–2 Roadmap for Upgrading Oracle Entitlements Server Client 11.1.2.x.x to 11.1.2.2.0

Sl No	Task	For More Information
1	Stop all the security module instances, and the servers.	See, Stopping all Security Module Instances
2	Upgrade the Oracle Entitlements Server Client to 11.1.2.2.0.	See, Upgrade Oracle Entitlements Server Client to 11.1.2.2.0
3	Start the security modules.	See, Starting the Security Modules
4	Verify the Oracle Entitlements Server Client Server upgrade.	See, Verifying Oracle Entitlements Server Client Upgrade

6.2.2 Stopping all Security Module Instances

Bring down all security module instances, Administration Server, and Managed Servers.

The security module instances shuts down when the Administration Server and Managed Servers are shut down.

To stop the servers, see Section 6.1.3, "Shutting Down Administration Server and Oracle Entitlements Server Managed Servers".

6.2.3 Upgrade Oracle Entitlements Server Client to 11.1.2.2.0

To upgrade Oracle Entitlements Server Client, you must use the 11.1.2.2.0 installer. During the procedure, point the Middleware Home to your existing 11.1.2.x.x Oracle Entitlements Server Client Middleware Home. This upgrades your Middleware Home and Oracle Home from 11.1.2.x.x to 11.1.2.2.0.

This section contains the following topics:

- Prerequisites

- Obtaining the Software
- Installing Oracle Entitlements Server Client 11g Release 2 (11.1.2.2.0)
- Verifying the Installation

6.2.3.1 Prerequisites

You must install and configure Oracle Entitlements Server Administration Server, as described in Section 6.1.5, "Updating Oracle Entitlements Server Binaries to 11.1.2.2.0".

6.2.3.2 Obtaining the Software

For more information on obtaining Oracle Fusion Middleware 11*g* software, see *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.

6.2.3.3 Installing Oracle Entitlements Server Client 11*g* Release 2 (11.1.2.2.0)

For more information on installing Oracle Entitlements Server Client 11.1.2.2.0, see "Installing Oracle Entitlements Server Client" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

6.2.3.4 Verifying the Installation

To verify that your Oracle Entitlements Server Client install was successful, go to your Oracle Home directory which you specified during installation and verify that the Oracle Entitlements Server Client installation files are created.

6.2.4 Starting the Security Modules

You must start the security modules by starting the Administration Server and Managed Servers.

To start the servers, see Section 6.1.9, "Starting the Administration Server and the Managed Servers".

6.2.5 Verifying Oracle Entitlements Server Client Upgrade

To verify, create an authorization, as mentioned in "Using the PEP API" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*, and see if it works correctly.

The Application Runtime Authorization continues working.

7

Upgrading Oracle Privileged Account Manager 11*g* Release 2 (11.1.2.x.x) Environments

This chapter describes how to upgrade Oracle Privileged Account Manager (OPAM) 11*g* Release 2 (11.1.2.1.0) and 11*g* Release 2 (11.1.2) environments to Oracle Privileged Account Manager 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

Note: For information about upgrading Oracle Privileged Account Manager on IBM WebSphere, see "Upgrading Oracle Privileged Account Manager on IBM WebSphere" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

Note: This chapter refers to Oracle Privileged Account Manager 11*g* Release 2 (11.1.2) and 11*g* Release 2 (11.1.2.1.0) environments as 11.1.2.x.x.

This chapter includes the following sections:

- Section 7.1, "Upgrade Roadmap for Oracle Privileged Account Manager"
- Section 7.2, "Reviewing System Requirements and Certification"
- Section 7.3, "Exporting the Pre-Upgrade Data"
- Section 7.4, "Stopping the Administration Servers and the Managed Server(s)"
- Section 7.5, "Upgrading Oracle WebLogic Server to 10.3.6"
- Section 7.6, "Updating Oracle Privileged Account Manager Binaries to 11.1.2.2.0"
- Section 7.7, "Upgrading the Database Schemas"
- Section 7.8, "Start the Administration Server and the Managed Server(s)"
- Section 7.9, "Redeploying the Applications"
- Section 7.10, "Enabling TDE or Non-TDE Mode in OPAM Data Store"
- Section 7.11, "Importing the Pre-Upgrade Data"
- Section 7.12, "Clearing Pre-Upgrade OPSS Artifacts"
- Section 7.13, "Optional: Configuring the Oracle Privileged Account Manager 11.1.2.2.0 Session Manager"
- Section 7.14, "Optional: Configuring Oracle Identity Navigator Application on OPAM Managed Server"

- Section 7.15, "Verifying the Oracle Privileged Account Manager Upgrade"

7.1 Upgrade Roadmap for Oracle Privileged Account Manager

Table 7–1 lists the tasks to be performed to upgrade Oracle Privileged Account Manager 11.1.2.x.x to Oracle Privileged Account Manager 11.1.2.2.0.

Table 7–1 Roadmap for Upgrading Oracle Privileged Account Manager 11.1.2.x.x to 11.1.2.2.0

Sl No	Task	For More Information
1	Review system requirements and certifications.	See, Reviewing System Requirements and Certification
2	If you are upgrading Oracle Privileged Account Manager 11.1.2 to Oracle Privileged Account Manager 11.1.2.2.0, you must export the pre-upgrade data. If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to Oracle Privileged Account Manager 11.1.2.2.0, skip this task.	See, Section 7.3, "Exporting the Pre-Upgrade Data"
3	Stop the Administration Server and all the Managed Servers.	See, Stopping the Administration Servers and the Managed Server(s)
4	If you are not using Oracle WebLogic Server 10.3.6, and you must upgrade Oracle WebLogic Server to 10.3.6.	See, Upgrading Oracle WebLogic Server to 10.3.6
5	Upgrade the Oracle Privileged Account Manager binaries to 11.1.2.2.0.	See, Updating Oracle Privileged Account Manager Binaries to 11.1.2.2.0
6	Upgrade the 11.1.2.x.x Database schemas.	See, Upgrading the Database Schemas
7	Start all the servers.	See, Start the Administration Server and the Managed Server(s)
8	Redeploy the Oracle Identity Navigator and Oracle Privileged Account Manager applications.	See, Redeploying the Applications
9	If you are upgrading Oracle Privileged Account Manager 11.1.2 to Oracle Privileged Account Manager 11.1.2.2.0, you must set up either TDE mode or non-TDE mode in the OPAM Data Store. If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to Oracle Privileged Account Manager 11.1.2.2.0, skip this task.	See, Enabling TDE or Non-TDE Mode in OPAM Data Store

Table 7–1 (Cont.) Roadmap for Upgrading Oracle Privileged Account Manager 11.1.2.x.x to 11.1.2.2.0

Sl No	Task	For More Information
10	If you are upgrading Oracle Privileged Account Manager 11.1.2 to Oracle Privileged Account Manager 11.1.2.2.0, you must import the pre-upgrade data. If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to Oracle Privileged Account Manager 11.1.2.2.0, skip this task.	See, Importing the Pre-Upgrade Data
11	If you are upgrading Oracle Privileged Account Manager 11.1.2 to Oracle Privileged Account Manager 11.1.2.2.0, you must clear the pre-upgrade OPSS artifacts. If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to Oracle Privileged Account Manager 11.1.2.2.0, skip this task.	See, Clearing Pre-Upgrade OPSS Artifacts
12	Configure the Oracle Privileged Account Manager session manager (if required).	See, Optional: Configuring the Oracle Privileged Account Manager 11.1.2.2.0 Session Manager
13	Configure the Oracle Identity Navigator application (if required).	See, Optional: Configuring Oracle Identity Navigator Application on OPAM Managed Server
14	Verify the upgrade.	See, Verifying the Oracle Privileged Account Manager Upgrade

7.2 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see Section 2.1, "Reviewing System Requirements and Certification".

7.3 Exporting the Pre-Upgrade Data

If you are upgrading Oracle Privileged Account Manager 11.1.2 to 11.1.2.2.0, you must export the pre-upgrade Oracle Privileged Account Manager data before you start the upgrade process.

> **Note:** If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to 11.1.2.2.0, skip this task.

You must export the pre-upgrade OPAM data such as targets, accounts, and users, before you upgrade Oracle Privileged Account Manager 11.1.2 to 11.1.2.2.0. The steps provided in this section describes the process to export the OPAM data to an XML file. A manual export is required because the back end data store will be moved from the OPSS schema to a native OPAM data store in the new version.

Use the following procedure to export the OPAM data:

1. Set the following environment variables:

Variable	Description
ORACLE_HOME	Where Oracle Privileged Account Manager is installed.
JAVA_HOME	Location of JDK used for the WebLogic installation.

2. Navigate to *ORACLE_HOME*/opam/bin.
3. Execute the following command with all the parameters mentioned:

   On UNIX:

```
./opam.sh
[-url <OPAM server url>]] (defaults to https://localhost:18102/opam)
-u [user name] (the user should have OPAM_SECURITY_ADMIN and OPAM_USER_MANAGER
roles)
-p <password>
-x export -f [export xml file]
[-encpassword <encryption/decryption password>] (provide a value for
encpassword for better security)
[-enckeylen <Key Length for encryption/decryption of password>] (defaults to
128)
[-log <log file Location>] (defaults to opamlog_<timestamp>.txt)
```

   On Windows:

```
./opam.bat
[-url <OPAM server url>]] (defaults to https://localhost:18102/opam)
-u [user name] (the user should have OPAM_SECURITY_ADMIN and OPAM_USER_MANAGER
roles)
-p <password>
-x export -f [export xml file]
[-encpassword <encryption/decryption password>] (provide a value for
encpassword for better security)
[-enckeylen <Key Length for encryption/decryption of password>] (defaults to
128)
[-log <log file Location>] (defaults to opamlog_<timestamp>.txt)
```

> **Note:** If the data was exported without an encryption password, then specify this with the parameter "`-noencrypt true`" while importing the data.

7.4 Stopping the Administration Servers and the Managed Server(s)

The upgrade process involves changes to the binaries and to the schema. So, before you begin the upgrade process, you must shut down the WebLogic Administration Server and the Oracle Privileged Account Manager Managed Server(s).

For information about stopping the WebLogic Administration Server and the Managed Servers, see Section 2.8, "Stopping the Servers".

7.5 Upgrading Oracle WebLogic Server to 10.3.6

Oracle Identity and Access Management 11.1.2.2.0 is certified with Oracle WebLogic Server 11*g* Release 1 (10.3.6). Therefore, if your existing Oracle Privileged Account Manager environment is using Oracle WebLogic Server 10.3.5 or the previous versions, you must upgrade Oracle WebLogic Server to 10.3.6.

For information about upgrading Oracle WebLogic Server to 10.3.6, see Section 2.3, "Upgrading to Oracle WebLogic Server 10.3.6".

7.6 Updating Oracle Privileged Account Manager Binaries to 11.1.2.2.0

To update Oracle Privileged Account Manager 11.1.2.x.x binaries to 11.1.2.2.0, you must use the Oracle Identity and Access Management 11.1.2.2.0 Installer. During the procedure, point the Middleware Home to your existing 11.1.2.x.x Oracle Privileged Account Manager Middleware Home. Your Oracle Home is upgraded from 11.1.2.x.x to 11.1.2.2.0.

For information about updating the Oracle Privileged Account Manager binaries to 11.1.2.2.0, see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

7.7 Upgrading the Database Schemas

Upgrade the following schemas using the Patch Set Assistant.

- OPAM
- OPSS - OPSS is selected as a dependency when you select OPAM.

For information about upgrading schemas using Patch Set Assistant, see Section 2.6, "Upgrading Schemas Using Patch Set Assistant".

After you upgrade the OPAM and OPSS schemas, the version of the OPAM schema will be 11.1.2.2.0.

7.8 Start the Administration Server and the Managed Server(s)

After you upgrade the schemas, start the WebLogic Administration Server and the Oracle Privileged Account Manager Managed Server(s).

For information about starting the WebLogic Administration Server and the Managed Servers, see Section 2.9, "Starting the Servers".

7.9 Redeploying the Applications

After you start the WebLogic Administration Server and the Oracle Privileged Account Manager Managed Servers, you must redelpoy the Oracle Identity Navigator and Oracle Privileged Account Manager applications. To do this, complete the following tasks:

- Redeploying Oracle Identity Navigator Application
- Redeployng Oracle Privileged Account Manager Application

7.9.1 Redeploying Oracle Identity Navigator Application

> **Note:** The Oracle Identity Navigator version number is 11.1.1.3.0 while the actual Oracle Identity Navigator version number should be 11.1.2.2.0.
>
> This is not an error. The discrepancy is caused by a difference between how Oracle Identity Navigator and Oracle Identity and Access Management releases are tracked internally.

Upgrading Oracle Identity Navigator redeploys Oracle Identity Navigator using `oinav.ear` for Oracle Identity Navigator 11.1.2.2.0 release. There are two ways of redeploying the `oinav.ear` - using the WebLogic Administration console, and using the WebLogic Scripting Tool.

Redeploy Oracle Identity Navigator applications using one of the following ways:

- Upgrading oinav Using WebLogic Server Administration Console
- Upgrading oinav Using WebLogic Scripting Tool (WLST)

Upgrading oinav Using WebLogic Server Administration Console

Complete the following steps to upgrade Oracle Identity Navigator through the WebLogic Administration console:

1. Log in to WebLogic Administration console:

   `http://admin_server_host:admin_server_port/console`

2. Under Domain Structure, click **Deployments**.
3. Select **oinav (11.1.1.3.0)** from the **Name** table.
4. Click **Update** and click **Finish** in the **Update Application Assistant** screen after verifying the source path.

> **Note:** If WebLogic is running in production mode, click **Lock & Edit** before clicking **Update.**

Upgrading oinav Using WebLogic Scripting Tool (WLST)

Complete the following steps to upgrade Oracle Identity Navigator through the WLST console:

On UNIX

1. Move from your present working directory to the *MW_HOME*`/wlserver_10.3/common/bin` directory by running the following command on the command line:

   `cd MW_HOME/wlserver_10.3/common/bin`

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   `./wlst.sh`

3. Connect to the Administration Server using the following command:

   `connect('weblogic-username','weblogic-password','weblogic-url')`

4. At the WLST prompt, run the following command:

```
redeploy('oinav#11.1.1.3.0')
```

5. Exit the WLST console using the `exit()` command.

On Windows

1. Move from your present working directory to the *MW_HOME*`\wlserver_10.3\common\bin` directory by running the following command on the command line:

   ```
   cd MW_HOME\wlserver_10.3\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following command:

   ```
   redeploy('oinav#11.1.1.3.0')
   ```

5. Exit the WLST console using the `exit()` command.

7.9.2 Redeployng Oracle Privileged Account Manager Application

> **Note:** The OPAM application version number is 11.1.2.0.0 while the actual Oracle Privileged Account Manager version number should be 11.1.2.2.0.
>
> This is not an error. The discrepancy is caused by a difference between how OPAM and Identity Access Management releases are tracked internally.

Upgrading Oracle Privileged Account Manager redeploys Oracle Privileged Account Manager using `opam.ear` for Oracle Privileged Account Manager 11.1.2.2.0 release. There are two ways of redeploying the `opam.ear` - using the WebLogic Administration console, and using the WebLogic Scripting Tool.

Redeploy Oracle Privileged Account Manager applications using one of the following ways:

- Upgrading opam Using WebLogic Server Administration Console
- Upgrading opam Using WebLogic Scripting Tool (WLST)

Upgrading opam Using WebLogic Server Administration Console

Complete the following steps to upgrade Oracle Privileged Account Manager through the WebLogic Administration console:

1. Log in to WebLogic Administration console:

   ```
   http://admin_server_host:admin_server_port/console
   ```

2. Under Domain Structure, click **Deployments**.
3. Select **opam (11.1.2.0.0)** from the **Name** table.
4. Click **Update** and click **Finish** in the **Update Application Assistant** screen after verifying the source path.

Note: If WebLogic is running in production mode, click **Lock & Edit** before clicking **Update.**

Upgrading opam Using WebLogic Scripting Tool (WLST)

Complete the following steps to upgrade Oracle Privileged Account Manager through the WLST console:

On UNIX

1. Move from your present working directory to the *MW_HOME*/wlserver_10.3/common/bin directory by running the following command on the command line:

   ```
   cd MW_HOME/wlserver_10.3/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following command:

   ```
   redeploy('opam#11.1.2.0.0')
   ```

5. Exit the WLST console using the `exit()` command.

On Windows

1. Move from your present working directory to the *MW_HOME*\wlserver_10.3\common\bin directory by running the following command on the command line:

   ```
   cd MW_HOME\wlserver_10.3\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following command:

   ```
   redeploy('opam#11.1.2.0.0')
   ```

5. Exit the WLST console using the `exit()` command.

7.10 Enabling TDE or Non-TDE Mode in OPAM Data Store

If you are upgrading Oracle Privileged Account Manager 11.1.2 to 11.1.2.2.0, you must enable TDE or non-TDE mode in the Oracle Privileged Account Manager data store.

Note: If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to 11.1.2.2.0, skip this task.

Oracle Privileged Account Manager can operate with Oracle Database TDE (Transparent Data Encryption) mode. You can choose to either enable or disable the TDE mode. Oracle strongly recommends to enable the TDE mode for enhanced

security. Depending upon what mode you wish to enable, complete one of the following tasks:

- Configuring TDE Mode in Data Store
- Configuring Non-TDE Mode in Data Store

7.10.1 Configuring TDE Mode in Data Store

To enable TDE mode in Oracle Privileged Account Manager data store, complete the following steps:

1. Enabling TDE in the Database
2. Enabling Encryption in OPAM Schema

7.10.1.1 Enabling TDE in the Database

For information about enabling Transparent Data Encryption (TDE) in the database for Oracle Privileged Account Manager, refer to the "Enabling Transparent Data Encryption" topic in *Oracle Database Advanced Security Administrator's Guide*.

For more information, see "Securing Stored Data Using Transparent Data Encryption" in the *Oracle Database Advanced Security Administrator's Guide*

After enabling TDE in the database for Oracle Privileged Account Manager, you must enable encryption in OPAM schema, as described in "Enabling Encryption in OPAM Schema" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

7.10.1.2 Enabling Encryption in OPAM Schema

To enable encryption in the OPAM schema, run the `opamxencrypt.sql` script with the OPAM schema user, using sqlplus or any other client.

```
IAM_HOME/opam/sql/opamxencrypt.sql
```

Example:

```
sqlplus DEV_OPAM/welcome1 @IAM_HOME/opam/sql/opamxencrypt.sql
```

7.10.2 Configuring Non-TDE Mode in Data Store

Note: This step is only necessary if you did not enable TDE as described in Section 7.10.1, "Configuring TDE Mode in Data Store".

While it is not recommended, if non-TDE mode is required by the user, the flag "tdemode" must be set to `false`. For more information, see "Setting Up Non-TDE Mode" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Caution: Oracle recommends that you always use Transparent Data Encryption(TDE). Without TDE, your data is not secure.

For more information on switching between the two modes, see "Securing Data On Disk" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.

7.11 Importing the Pre-Upgrade Data

If you are upgrading Oracle Privileged Account Manager 11.1.2 to 11.1.2.2.0, you must export the pre-upgrade Oracle Privileged Account Manager data after you upgrade to 11.1.2.2.0.

> **Note:** If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to 11.1.2.2.0, skip this task.

To import the pre-upgrade OPAM data, do the following:

1. Set the following environment variables:

Variable	Description
ORACLE_HOME	Oracle Privileged Account Manager is installed.
JAVA_HOME	Location of JDK used for the WebLogic installation.

2. Navigate to *ORACLE_HOME*/opam/bin.
3. Execute the opam.sh script with the following parameters:

```
./opam.sh
-url <OPAM server url> (defaults to https://localhost:18102/opam)
-u <user name> (the user should have OPAM_SECURITY_ADMIN and OPAM_USER_MANAGER
roles)
-p <password>
-x import -f <import xml file>
-encpassword <encryption/decryption password>
-enckeylen <Key Length for encryption/decryption of password> (Defaults to 128)
-log <log file Location> (defaults to opamlog_<timestamp>.txt)
```

7.12 Clearing Pre-Upgrade OPSS Artifacts

If you are upgrading Oracle Privileged Account Manager 11.1.2 to 11.1.2.2.0, you must clear the pre-upgrade OPSS artifacts after you upgrade to 11.1.2.2.0.

> **Note:** If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to 11.1.2.2.0, skip this task.

To clear the OPSS artifacts of the pre-upgrade instance, do the following:

On UNIX:

```
$ORACLE_HOME/common/bin/wlst.sh $ORACLE_HOME/opam/config/clean-opss.py <WebLogic
Administrator Username> <WebLogic Administrator Password>
<t3://<adminserver-host>:<adminserver-port>
```

On Windows:

```
$ORACLE_HOME\common\bin\wlst.cmd $ORACLE_HOME\opam\config\clean-opss.py <WebLogic
Administrator Username> <WebLogic Administrator Password>
<t3://<adminserver-host>:<adminserver-port>
```

7.13 Optional: Configuring the Oracle Privileged Account Manager 11.1.2.2.0 Session Manager

If you wish to configure the Oracle Privileged Account Manager 11.1.2.2.0 session manager, complete the following steps:

1. Stop the WebLogic Administration Server and the Oracle Privileged Account Manager Managed Servers.

   For information about stopping the servers, see Section 7.4, "Stopping the Administration Servers and the Managed Server(s)".

2. Run the WLST script `configureSessionManager.py` from the location *`ORACLE_HOME`*`/opam/tools` as shown in the following example:

   On UNIX:

   ```
   ./wlst.sh ORACLE_HOME/opam/tools/configureSessionManager.py  -d <Path_to_WebLogic_Domain_Directory> -o <Path_to_Oracle_Home_Directory>
   ```

   On Windows:

   ```
   wlst.cmd ORACLE_HOME\opam\tools\configureSessionManager.py  -d <Path_to_WebLogic_Domain_Directory> -o <Path_to_Oracle_Home_Directory>
   ```

7.14 Optional: Configuring Oracle Identity Navigator Application on OPAM Managed Server

If you wish to configure Oracle Identity Navigator on the Oracle Privileged Account Manager Managed Server, complete the following steps:

1. Stop the servers.
2. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

3. Run the following command to launch the Oracle Fusion Middleware configuration wizard:

   On UNIX:

   ```
   ./config.sh
   ```

   On Windows:

   ```
   config.cmd
   ```

4. Select the **Extend an existing WebLogic domain** option, and select the OPAM domain.
5. Select **Oracle Identity Navigator for Managed Server** from the products. Select **Keep existing component** option whenever it detects a conflict in the wizard.
6. Complete the configuration. Oracle Identity Navigator will run on the Oracle Privileged Account Manager Managed Server after starting the servers.

7.15 Verifying the Oracle Privileged Account Manager Upgrade

Verify the Oracle Privileged Account Manager upgrade by doing the following:

1. Log in to the Oracle Privileged Account Manager 11.1.2.2.0 console using the following URL:

   `http://adminserver_host:adminserver_port/oinav/opam`

   If you have configured Oracle Identity Navigator on the Oracle Privileged Account Manager Managed Server, you can also use the following URL to log in to the Oracle Privileged Account Manager 11.1.2.2.0 console:

   `http://opamserver_host:opamserver_nonssl_port/oinav/opam`

2. Verify that the pre-upgrade data, targets, accounts, grants are present, and working as expected.

8

Upgrading Oracle Identity Navigator 11*g* Release 2 (11.1.2.x.x) Environments

This chapter describes how to upgrade Oracle Identity Navigator 11*g* Release 2 (11.1.2.1.0) and 11*g* Release 2 (11.1.2) environments to Oracle Identity Navigator 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

> **Note:** This chapter refers to Oracle Identity Navigator 11*g* Release 2 (11.1.2) and 11*g* Release 2 (11.1.2.1.0) environments as 11.1.2.x.x.

This chapter includes the following sections:

- Section 8.1, "Upgrade Roadmap for Oracle Identity Navigator"
- Section 8.2, "Reviewing System Requirements and Certification"
- Section 8.3, "Exporting Oracle Identity Navigator 11.1.2.x.x Metadata"
- Section 8.4, "Shutting Down Administration Server and Managed Servers"
- Section 8.5, "Upgrading Oracle WebLogic Server to 10.3.6"
- Section 8.6, "Updating Oracle Identity Navigator Binaries to 11.1.2.2.0"
- Section 8.7, "Creating Oracle Platform Security Services Schema"
- Section 8.8, "Extending Oracle Identity Navigator 11.1.2.x.x Component Domains with Oracle Platform Security Services Template"
- Section 8.9, "Upgrading Oracle Platform Security Services"
- Section 8.10, "Configuring Database Security Store"
- Section 8.11, "Starting the WebLogic Administration Server"
- Section 8.12, "Verifying the Deployment Summary"
- Section 8.13, "Upgrading Oracle Identity Navigator Application"
- Section 8.14, "Importing the Oracle Identity Navigator 11.1.2.2.0 Metadata"
- Section 8.15, "Verifying the Upgrade"
- Section 8.16, "Optional: Configuring Oracle Identity Manager on the Oracle Privileged Account Manager Managed Server from the Administration Server"

8.1 Upgrade Roadmap for Oracle Identity Navigator

Note: If you do not follow the exact sequence provided in this task table, your Oracle Identity Navigator upgrade may not be successful.

Table 8–1 lists the steps to upgrade Oracle Identity Navigator 11.1.2.x.x to 11.1.2.2.0.

Table 8–1 Roadmap for Upgrading Oracle Identity Navigator 11.1.2.x.x to 11.1.2.2.0.

So. No.	Task	For More Information
1	Review system requirements and certifications.	See, Reviewing System Requirements and Certification
2	Export Oracle Identity Navigator data.	See, Exporting Oracle Identity Navigator 11.1.2.x.x Metadata
3	Shut down all servers. This includes both Administration Server and Managed Servers.	See, Shutting Down Administration Server and Managed Servers
4	Optional - Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6.	See, Upgrading Oracle WebLogic Server to 10.3.6
5	Upgrade 11.1.2.x.x Oracle Home to 11.1.2.2.0.	See, Updating Oracle Identity Navigator Binaries to 11.1.2.2.0
6	Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load OPSS schema for Oracle Identity and Access Management products.	See, Creating Oracle Platform Security Services Schema
7	Extend your Oracle Identity Navigator 11.1.2.x.x domain with the OPSS template.	See, Extending Oracle Identity Navigator 11.1.2.x.x Component Domains with Oracle Platform Security Services Template
8	Upgrade Oracle Platform Security Services.	See, Upgrading Oracle Platform Security Services
9	Run the `configuresecuritystore.py` script to configure policy stores.	See, Configuring Database Security Store
10	Start the Administration Server.	See, Starting the WebLogic Administration Server
11	Verify the deployments summary.	See, Verifying the Deployment Summary
12	Upgrade Oracle Identity Navigator.	See, Upgrading Oracle Identity Navigator Application
13	Import data.	See, Importing the Oracle Identity Navigator 11.1.2.2.0 Metadata
14	Verify the Oracle Identity Navigator upgrade.	See, Verifying the Upgrade
15	Optional - Configure Oracle Identity Manager on the Oracle Privileged Account Manager Managed Server from the Administration Server	See, Optional: Configuring Oracle Identity Manager on the Oracle Privileged Account Manager Managed Server from the Administration Server

8.2 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see Section 2.1, "Reviewing System Requirements and Certification".

8.3 Exporting Oracle Identity Navigator 11.1.2.x.x Metadata

Oracle Identity Navigator uses MDS as its metadata store. During upgrade, when you update the application, the metadata gets overwritten. Therefore, you need to export it and keep it in a temporary location so that it can be used to import original metadata after upgrade.

On the computer where Oracle Identity Navigator 11.1.2.x.x is installed, export the Oracle Identity Navigator metadata to an export directory using WLST as follows:

On UNIX:

1. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST (online) command:

   ```
   exportMetadata(application='oinav',server='AdminServer',toLocation='exp
   ort_directory')
   ```

   where

   `export_directory` is the directory where you want to export Oracle Identity Navigator metadata to.

On Windows:

1. Move from your present working directory to the `<IAM_HOME>\common\bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST (online) command:

   ```
   exportMetadata(application='oinav',server='AdminServer',toLocation='exp
   ort_directory')
   ```

   where

   `export_directory` is the directory where you want to export Oracle Identity Navigator metadata to.

8.4 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. So, before you begin the upgrade process, you must shut down the Oracle Identity Navigator Managed Server(s) and the WebLogic Administration Server.

For information about stopping the WebLogic Administration Server and the Managed Server(s), see Section 2.8, "Stopping the Servers".

8.5 Upgrading Oracle WebLogic Server to 10.3.6

Oracle Identity and Access Management 11.1.2.2.0 is certified with Oracle WebLogic Server 11*g* Release 1 (10.3.6). Therefore, if your existing Oracle Identity Navigator environment is using Oracle WebLogic Server 10.3.5 or the previous versions, you must upgrade Oracle WebLogic Server to 10.3.6.

For information about upgrading Oracle WebLogic Server to 10.3.6, see Section 2.3, "Upgrading to Oracle WebLogic Server 10.3.6".

8.6 Updating Oracle Identity Navigator Binaries to 11.1.2.2.0

To upgrade Oracle Identity Navigator, you must use the Oracle Identity and Access Management 11.1.2.2.0 Installer. During the procedure, point the Middleware Home to your existing 11.1.2.x.x Oracle Identity Navigator Middleware Home. Your Oracle Home is upgraded from 11.1.2.x.x to 11.1.2.2.0.

For information about updating the Oracle Identity Navigator binaries to 11.1.2.2.0, see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

8.7 Creating Oracle Platform Security Services Schema

You must create Oracle Platform Security Services (OPSS) schema because Oracle Identity Navigator upgrade process involves OPSS schema policy store changes. The keys, roles, permissions, and other artifacts used by the applications must migrate to the policy store. To create schemas, you must use Repository Creation Utility.

For information about creating schemas using RCU, see Section 2.5, "Creating Database Schemas Using Repository Creation Utility".

Note: In the **Select Components** screen, expand **AS Common Schemas** and select **Oracle Platform Security Services**. The **Metadata Services** schema is selected automatically.

8.8 Extending Oracle Identity Navigator 11.1.2.x.x Component Domains with Oracle Platform Security Services Template

Oracle Identity Navigator 11.1.2.2.0 uses the database to store policies. This requires extending the 11.1.2.x.x Oracle Identity Navigator domain to include the OPSS data source.

To do so, complete the following steps:

1. Run the following command to launch the Oracle Fusion Middleware configuration wizard:

On UNIX:

```
./config.sh
```

It is located in the `<MW_HOME>/Oracle_IDM1/common/bin` directory.

On Windows:

```
config.cmd
```

It is located in the `<MW_HOME>\Oracle_IDM1\common\bin` directory.

2. On the **Welcome** screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
3. On the **Select a WebLogic Domain Directory** screen, browse to the directory that contains the WebLogic domain in which you configured the components. Click **Next**. The **Select Extension Source** screen is displayed.
4. On the **Select Extension Source** screen, select the **Oracle Platform Security Service - 11.1.1.0 [Oracle_IDM1]** option. After selecting the domain configuration options, click **Next**.
5. The **Configure JDBC Data Sources** screen is displayed. Configure the opss-DBDS data source, as required. After the test succeeds, the **Configure JDBC Component Schema** screen is displayed.
6. On the **Configure JDBC Component Schema** screen, select the **Oracle Platform Security Services** schema.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**.

   The **Test JDBC Component Schema** screen is displayed. After the test succeeds, the **Select Optional Configuration** screen is displayed.
7. On the **Select Optional Configuration** screen, you can configure Managed Servers, Clusters, and Machines and Deployments and Services. Do not select anything as you have already configured in your Oracle Identity Navigator 11.1.2.1.0 environment. Click **Next**.
8. On the **Configuration Summary** screen, review the domain configuration, and click **Extend** to start extending the domain.

Your existing Oracle Identity Navigator domain is extended to support Oracle Platform Security Services (OPSS).

8.9 Upgrading Oracle Platform Security Services

After you upgrade schemas, you must upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Identity Navigator to 11.1.2.2.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see Section 2.7, "Upgrading Oracle Platform Security Services".

8.10 Configuring Database Security Store

You must configure the Database Security Store as it is the only security store type supported by Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0).

For more information on configuring Oracle Platform Security Services, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

8.11 Starting the WebLogic Administration Server

After the upgrade is complete, start the WebLogic Administration Server, the Administration Server that contains the Oracle Identity Navigator console.

For information about starting the WebLogic Administration Server, see Section 2.9.2, "Starting the WebLogic Administration Server".

8.12 Verifying the Deployment Summary

To verify the deployment summary, do the following:

1. Log in to the WebLogic Administration console:

   ```
   http://<admin server host>:<admin server port>/console
   ```

2. Under Domain Structure, click **Deployments**. The Summary of Deployments page is displayed.
3. Check the summary details and verify that **oinav (11.1.1.3.0)** is present in the Name table.

8.13 Upgrading Oracle Identity Navigator Application

Note: The Oracle Identity Navigator version number is 11.1.1.3.0 while the Oracle Identity Navigator version number is 11.1.2.2.0.

This is not an error. The discrepancy is caused by a difference between how Oracle Identity Navigator and Identity Access Management releases are tracked internally.

Upgrading Oracle Identity Navigator redeploys Oracle Identity Navigator using `oinav.ear` for Oracle Identity Navigator 11.1.2.2.0 release. There are two ways of redeploying the `oinav.ear`:

- Upgrading `oinav` using the WebLogic Server Administration Console.
- Upgrading `oinav` using the WebLogic Scripting Tool (WLST).

Using WebLogic Server Administration Console

Complete the following steps to upgrade Oracle Identity Navigator through the WebLogic Administration console:

1. Log in to WebLogic Administration console:

   ```
   http://<admin server host>:<admin server port>/console
   ```

2. Under Domain Structure, click **Deployments**.
3. Select **oinav (11.1.1.3.0)** from the **Name** table.
4. Click **Update** and click **Finish** in the **Update Application Assistant** screen after verifying the source path.

Note: If WebLogic is running in production mode, click **Lock & Edit** before clicking **Update.**

Using WebLogic Scripting Tool (WLST)

Complete the following steps to upgrade Oracle Identity Navigator through the WLST console:

On UNIX

1. Move from your present working directory to the `<MW_HOME>/wlserver_10.3/common/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/wlserver_10.3/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   connect('weblogic-username','weblogic-password','weblogic-url')

4. At the WLST prompt, run the following command:

   ```
   redeploy('oinav#11.1.1.3.0')
   ```

5. Exit the WLST console using the `exit()` command.

On Windows

1. Move from your present working directory to the `<MW_HOME>\wlserver_10.3\common\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\wlserver_10.3\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   connect('weblogic-username','weblogic-password','weblogic-url')

4. At the WLST prompt, run the following command:

   ```
   redeploy('oinav#11.1.1.3.0')
   ```

5. Exit the WLST console using the `exit()` command.

8.14 Importing the Oracle Identity Navigator 11.1.2.2.0 Metadata

You must import the metadata which was exported earlier so that Oracle Identity Navigator gets back the metadata present before upgrade. Import Oracle Identity Navigator 11.1.2.2.0 metadata by running the following WLST command:

On UNIX:

1. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST (online) command:

   ```
   importMetadata(application='oinav',server='AdminServer',fromLocation='e
   xport_directory')
   ```

   where

   `export_directory` is the directory where you have exported the Oracle Identity Navigator metadata to.

On Windows:

1. Move from your present working directory to the `<IAM_HOME>\common\bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST (online) command:

   ```
   importMetadata(application='oinav',server='AdminServer',fromLocation='e
   xport_directory')
   ```

   where

   `export_directory` is the directory where you have exported Oracle Identity Navigator metadata to.

> **Note:** Oracle Business Intelligence Publisher 10*g* report format is not supported in Oracle Identity Navigator 11.1.2.2.0 release. It is not mandatory, but if you want to remove the reports, see "Configuring Oracle Business Intelligence Publisher" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.

8.15 Verifying the Upgrade

To verify the Oracle Identity Navigator upgrade, do the following:

1. Log in to the Oracle Identity Navigator console:

   ```
   http://<admin server host>:<admin server port>/oinav
   ```

2. In the Dashboard page, check for the version number in the bottom right corner.

   The version number should be 11.1.2.2.0.

8.16 Optional: Configuring Oracle Identity Manager on the Oracle Privileged Account Manager Managed Server from the Administration Server

To configure Oracle Identity Navigator on the Oracle Privileged Account Manager managed server from the administration server, do the following:

1. Stop the servers.
2. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

3. Run the following command to launch the Oracle Fusion Middleware configuration wizard:

   ```
   ./config.sh
   ```

   It is located in the `<MW_HOME>/Oracle_IDM1/common/bin` directory.
4. Select **Keep existing content** whenever it detects a conflict in the wizard.
5. Complete the configuration. Oracle Identity Navigator will run on the managed server after starting the servers.

Part III

Upgrading Oracle Identity and Access Management 11*g* Release 1 (11.1.1.x.x) and 9.x Environments

This part includes the following chapters:

- Chapter 9, "Upgrading Oracle Access Manager 11g Release 1 (11.1.1.x.x) Environments"
- Chapter 10, "Upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x) Environments"
- Chapter 11, "Upgrading Oracle Identity Manager 11g Release 1 (11.1.1.x.x) Environments"
- Chapter 12, "Upgrading Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) Environment"
- Chapter 13, "Upgrading Oracle Identity Navigator 11g Release 1 (11.1.1.x.x) Environments"
- Chapter 14, "Upgrading Oracle Identity Manager 9.1.x.x Environments"

9

Upgrading Oracle Access Manager 11*g* Release 1 (11.1.1.x.x) Environments

This chapter describes how to upgrade your existing Oracle Access Manager 11*g* Release 1 (11.1.1.5.0) and 11*g* Release 1 (11.1.1.7.0) environments to Oracle Access Management Access Manager (Access Manager) 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

> **Note:** This chapter refers to Oracle Access Manager 11g Release 1 (11.1.1.5.0) and 11g Release 1 (11.1.1.7.0) environments as 11.1.1.x.x.

This chapter includes the following sections:

- Upgrade Roadmap for Oracle Access Manager
- Reviewing System Requirements and Certification
- Shutting Down Administration Server and Managed Servers
- Backing Up Oracle Access Manager 11g Release 1 (11.1.1.x.x)
- Upgrading Oracle WebLogic Server
- Creating Oracle Access Management Access Manager Schemas Using Repository Creation Utility
- Upgrading Oracle Access Manager Binaries to 11.1.2.2.0
- Extending Oracle Access Manager 11.1.1.x.x Component Domains with Oracle Platform Security Services Template
- Upgrading Oracle Platform Security Services Schemas
- Upgrading Oracle Platform Security Services
- Configuring Oracle Platform Security ServicesSecurity Store
- Exporting Access Data
- Importing Access Data
- Copying Modified System mbean Configurations
- Starting the Administration Server and Access Manager Managed Servers
- Redeploying Oracle Access Management Access Manager Servers and Shared Libraries
- Stopping the Administration Server and Access Manager Managed Servers
- Deleting Folders

- Upgrading System Configuration
- Starting the Administration Server and Access Manager Managed Servers
- Verifying the Upgrade
- Troubleshooting

9.1 Upgrade Roadmap for Oracle Access Manager

Note: If you do not follow the exact sequence provided in this task table, your Oracle Access Manager upgrade may not be successful.

Table 9–1 lists the steps to upgrade Oracle Access Manager 11.1.1.x.x.

Table 9–1 Upgrade Flow

Task No.	Task	For More Information
1	Review system requirements and certifications.	See, Reviewing System Requirements and Certification
2	Shut down all servers. This includes both Administration Server and Managed Servers.	See, Shutting Down Administration Server and Managed Servers
3	Back up your environment.	See, Backing Up Oracle Access Manager 11g Release 1 (11.1.1.x.x)
4	Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6.	See, Upgrading Oracle WebLogic Server
5	Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load Access Manager schemas and OPSS schema.	See, Creating Oracle Access Management Access Manager Schemas Using Repository Creation Utility
6	Upgrade 11.1.1.x.x Oracle Home to 11.1.2.2.0.	See, Upgrading Oracle Access Manager Binaries to 11.1.2.2.0
7	Extend your Oracle Access Manager 11.1.1.x.x domain with the OPSS template.	See, Extending Oracle Access Manager 11.1.1.x.x Component Domains with Oracle Platform Security Services Template
8	Upgrade the Oracle Platform Security Services schema.	See, Upgrading Oracle Platform Security Services Schemas
9	Upgrade Oracle Platform Security Services.	See, Upgrading Oracle Platform Security Services
10	Run the `configuresecuritystore.py` script to configure policy stores.	See, Configuring Oracle Platform Security ServicesSecurity Store
11	Export access data.	See, Exporting Access Data
12	Import access data.	See, Importing Access Data
13	Copy infrastructure mbean jar and configuration files	See, Copying Modified System mbean Configurations
14	Start the Administration Server and Oracle Access Management Access Manager Managed Servers.	See, Starting the Administration Server and Access Manager Managed Servers

Table 9–1 (Cont.) Upgrade Flow

Task No.	Task	For More Information
15	Redeploy Access Manager servers and shared libraries.	See, Redeploying Oracle Access Management Access Manager Servers and Shared Libraries
16	Stop the Administration Server and Oracle Access Management Access Manager Managed Server.	See, Stopping the Administration Server and Access Manager Managed Servers
17	Delete the `tmp` and `stage` folders.	See, Deleting Folders
18	Upgrade the system configuration of Oracle Access Manager.	See, Upgrading System Configuration
19	Start the Administration Server and Oracle Access Management Access Manager Managed Servers.	See, Starting the Administration Server and Access Manager Managed Servers
20	Verify the Access Manager upgrade.	See, Verifying the Upgrade

9.2 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements for the products you are installing or upgrading. For more information see Section 2.1, "Reviewing System Requirements and Certification".

9.3 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Administration Server and Managed Servers.

For information about stopping the servers, see "Stopping the Servers" on page 2-10.

9.4 Backing Up Oracle Access Manager 11g Release 1 (11.1.1.x.x)

You must back up your Oracle Access Manager 11.1.1.x.x environment before you upgrade to Access Manager 11.1.2.

After stopping the servers, back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Access Manager schemas
- MDS schemas
- Audit and any other dependent schemas

9.5 Upgrading Oracle WebLogic Server

You can upgrade WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6 by using the WebLogic 10.3.6 Upgrade Installer. For information about upgrading Oracle WebLogic Server, see "Upgrading to Oracle WebLogic Server 10.3.6" on page 2-2.

9.6 Creating Oracle Access Management Access Manager Schemas Using Repository Creation Utility

Upgrading Oracle Access Manager 11.1.1.x.x schema to Oracle Access Management Access Manager 11.1.2 is not supported. You cannot update Oracle Access Manager 11.1.1.x.x schemas to Access Manager 11.1.2, so, you must create new Access Manager 11.1.2 schemas.

Run Repository Creation utility (RCU) to create the Access Manager schema. Select all dependent schemas so that OPSS schema gets created too.

For more information, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

Note: Even if you are creating new schemas, do not delete your Oracle Access Manager 11.1.1.x.x schemas and do not use the old schema name, as you will need the old schema credentials while "Exporting Access Data".

9.7 Upgrading Oracle Access Manager Binaries to 11.1.2.2.0

To upgrade Oracle Access Manager, you must use the 11.1.2.2.0 installer. During the procedure, point the Middleware Home to your existing 11.1.1.x.x Oracle Access Manager Middleware Home. Your Oracle Home is upgraded from 11.1.1.x.x to 11.1.2.2.0.

Note: Before upgrading the Oracle Access Manager binaries to 11*g* Release 2 (11.1.2.2.0), you must ensure that the OPatch version in *ORACLE_HOME* and *MW_HOME*/oracle_common is 11.1.0.9.9. Different OPatch version might cause patch application failure. If you have upgraded opatch to a newer version, you will have to roll back to version 11.1.0.9.9.

For information about upgrading Oracle Access Manager 11g Release 1 (11.1.1.x.x) to Oracle Access Management Access Manager 11g Release 2 (11.1.2.2.0), see "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)" on page 2-2.

9.8 Extending Oracle Access Manager 11.1.1.x.x Component Domains with Oracle Platform Security Services Template

Oracle Access Management Access Manager 11.1.2.2.0 uses the database to store policies. This requires extending Oracle Access Manager 11.1.1.x.x domain to include the OPSS data source.

To extend your Oracle Access Manager 11.1.1.x.x component domain with the OPSS template, complete the following steps:

1. Run the following command:

   On UNIX:

   ./config.sh

   It is located in the <MW_HOME>/<Oracle_IDM1>/common/bin directory.

On Windows:

```
config.cmd
```

It is located in the <MW_HOME>\<Oracle_IDM1>\common\bin directory.

2. On the **Welcome** screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
3. On the **Select a WebLogic Domain Directory** screen, browse to the directory that contains the WebLogic domain in which you configured Oracle Access Manager. Click **Next**. The **Select Extension Source** screen appears.
4. On the **Select Extension Source** screen, select the **Oracle Platform Security Service - 11.1.1.0 [Oracle_IDM1]** option. After selecting the domain configuration options, click **Next**. The **Configure JDBC Component Schema** screen appears.
5. On the **Configure JDBC Component Schema** screen, do the following:
   - Select **OAM Infrastructure**, and update the Oracle Access Manager 11.1.1.x.x schema information with the Access Manager 11.1.2.2.0 schema details.
   - Select **OPSS Schema**, and specify the values for Schema Owner, Schema Password, Database and Service, Host Noame, and Port.
   - Click **Next**.

   The **Test JDBC Component Schema** screen appears. After the test succeeds, the **Select Optional Configuration** screen appears.
6. On the **Select Optional Configuration** screen, you can configure Managed Servers, Clusters, and Machines and Deployments and Services. Do not select anything as you have already configured your Oracle Access Manager 11.1.1.x.x environment. Click **Next**.
7. On the **Configuration Summary** screen, review the domain configuration, and click **Extend** to start extending the domain.

Your existing Oracle Access Manager domain is extended to support Oracle Platform Security Services (OPSS), and Oracle Access Manager is configured to use the newly created 11.1.2.2.0 OPSS policy schema.

9.9 Upgrading Oracle Platform Security Services Schemas

You must upgrade the Oracle Platform Security Services schemas using Patch Set Assistant. To do this, complete the following steps:

1. Start the Patch Set Assistant from the location *MW_HOME*/oracle_common/bin using the following command:

   ```
   ./psa
   ```

2. Select **opss**.
3. Specify the Database connection details, and select the schema to be upgraded.

After you upgrade Oracle Platform Security Services schema, verify the upgrade by checking the log file at the location *MW_HOME*/oracle_common/upgrade/logs/psa<*timestamp*>.log.

The *timestamp* refers to the actual date and time when Patch Set Assistant was run. If the upgrade fails, check the log files to rectify the errors and run the Patch Set Assistant again.

9.10 Upgrading Oracle Platform Security Services

After you upgrade schemas, you must upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Access Manager to 11.1.2.2.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see Section 2.7, "Upgrading Oracle Platform Security Services"

9.11 Configuring Oracle Platform Security ServicesSecurity Store

You must configure the Database Security Store as it is the only security store type supported by Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0).

For more information on configuring Oracle Platform Security Services, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

9.12 Exporting Access Data

Policy information from Oracle Access Manager 11.1.1.x.x schema needs to be extracted before importing it to the Access Manager 11.1.2.2.0 schema. The `exportAccessData` WLST command exports the Access Manager policy and configuration information from the 11.1.1.x.x Oracle Access Manager domain. You must export Oracle Access Manager 11.1.1.x.x configuration details, policy stores, keys, and CSF Passwords.

Note: Make sure to shutdown all WebLogic Server processes (administration server, Oracle Access Manager managed server, and node manager) before executing these export commands.

Complete the following steps to export data:

On UNIX:

1. Move from your present working directory to the `<MW_HOME>/<Oracle_IDM1>/common/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/<Oracle_IDM1>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. At the WLST prompt, run the following script:

   ```
   exportAccessData("<UPGRADE_PROPERTIES_FILE>")
   ```

   For example:

   ```
   exportAccessData("<ORACLE_HOME>/oam/server/wlst/scripts/sample_
   properties/oam_upgrade.properties")
   ```

   See Table 9–3 for sample properties and description.

4. Exit the WLST console using the `exit()` command.

On Windows:

1. Move from your present working directory to the `<MW_HOME>\<Oracle_IDM1>\common\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\<Oracle_IDM1>\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. At the WLST prompt, run the following script:

   ```
   exportAccessData("<UPGRADE_PROPERTIES_FILE>")
   ```

   For example:

   ```
   exportAccessData("<ORACLE_HOME>\\oam\\server\\wlst\\scripts\\sample_properties\\oam_upgrade-windows.properties")
   ```

   See Table 9–3 for sample properties and description.

4. Exit the WLST console using the `exit()` command.

Table 9–2 describes the parameters you must specify on the command line:

Table 9–2 Parameters for Exporting Data

Parameter	Description
`properties_location`	Specify the path to the `oam_upgrade.properties` file in the Access Manager 11.1.1.x.x installation. The following example shows the complete path: On UNIX, it is located in the `<ORACLE_HOME>/oam/server/wlst/scripts/sample_properties/oam_upgrade.properties` directory. On Windows, it is located in the `<ORACLE_HOME>\oam\server\wlst\scripts\sample_properties\oam_upgrade-windows.properties` directory.

Table 9–3 lists the properties of `oam_upgrade.properties`:

Table 9–3 Property Description

Properties	Description
`MW_HOME`	Specify the complete path to the Middleware Home. The following example shows the complete path: On UNIX, it is located in the `Oracle/Middleware` directory. On Windows, it is located in the `Oracle\\Middleware` directory.
`ORACLE_HOME`	This property refers to the location of the Oracle Identity and Access Management software. The following example shows the complete path: On UNIX, it is located in the `<MW_HOME>/<Oracle_IDM1>` directory. On Windows, it is located in the `<MW_HOME>\\<Oracle_IDM1>` directory.

Table 9–3 (Cont.) Property Description

Properties	Description
OAM_DOMAIN_HOME	This property refers to the existing Oracle Access Manager 11.1.1.x.x domain home. The following example shows the complete path: On UNIX, it is located in the <MW_HOME>/user_projects/domains/<oam_domain> directory. On Windows, it is located in the <MW_HOME>\\user_projects\\domains\\<oam_domain> directory.
ORACLE_COMMON_HOME	This property refers to the common components home. The following example shows the complete path: On UNIX, it is located in the <MW_HOME>/Oracle_Common directory. On Windows, it is located in the <MW_HOME>\\Oracle_Common directory.
OAM_DEST_ARTIFACTS_LOCATION	This property refers to the location where you want to place the upgrade artifacts, such as Oracle Access Manager 11.1.1.x.x configuration and policy files. **Note**: Make sure that the artifacts folder has read/write access.
OAM_TYPE_OF_UPGRADE	This is an InPlace upgrade.
OAM_IS_INCREMENTAL	This property is used to specify if you run the upgrade in an incremental mode. Incremental form of upgrade is not supported in Access Manager 11.1.2.2.0. Therefore, set the value as False.
OAM_POLICY_UPGRADE_OPTIMIZATION	As a part of the Oracle Access Manager policy upgrade, the changes to the out of the box Access Manager policies are applied on top of the existing (11.1.1.x.x) out of the box policies. This process involves a three way merge of the Access Manager policies. This is a time consuming process (takes about 30 minutes). If you want to proceed with the merge, set the property to False. If you want to replace the Oracle Access Manager 11.1.1.x.x out of the box policies with the new ones, without the merge process, set this property to True.
OAM_PS1_SCHEMA_OWNER	Use this property to connect to the 11.1.1.x.x policy store. Specify the Oracle Access Manager 11.1.1.x.x schema owner.
OAM_PS1_SCHEMA_CRED	Use this property to connect to the 11.1.1.x.x policy store. Specify the Oracle Access Manager 11.1.1.x.x schema credentials.
OAM_PS1_CREDENTIAL_ALIAS	Use this property to connect to the 11.1.1.x.x policy store. Specify the Oracle Access Manager 11.1.1.x.x Oracle Entitlements Server database credential alias as: OESDBCredentialAlias
OAM_PS1_JDBC_CONN_STRING	Use this property to connect to the 11.1.1.x.x policy store. Specify the JDBC connection string in the following format: jdbc:oracle:thin:@dbhost:dbport/sid
OAM_PS1_JDBC_DRIVER_CLASS	Use this property to connect to the 11.1.1.x.x policy store. Specify the JDBC driver class in the following format: oracle.jdbc.OracleDriver
OAM_PS1_ROOT_DN	Use this property to connect to the 11.1.1.x.x policy store. Specify the properties as: cn=farm,cn=JPSContext,cn=jpsroot

Table 9–3 (Cont.) Property Description

Properties	Description
OAM_PS1_POLICY_FILE	This property refers to the absolute path to the XML file where extracted 11.1.1.x.x policy needs to be saved. Specify the path where you want to save the extracted Oracle Access Manager 11.1.1.x.x policies. For example: On UNIX, specify the following path: OAM_PS1_POLICY_FILE=<UPGRADE_ATRIFACTS_DIR>/oam-policy-ps1.xml On Windows, specify the following path: OAM_PS1_POLICY_FILE=<UPGRADE_ATRIFACTS_DIR>\\oam-policy-ps1.xml
OAM_PS1_POLICY_JARS	Upgrade frameworks loads version specific jars for Exporting and Importing data. This property refers to the Oracle Access Manager 11.1.1.x.x policy jars available at the following path: On UNIX, it is located in the $<ORACLE_HOME>/oam/server/lib/upgrade/ps1-policy directory. On Windows, it is located in the <ORACLE_HOME>\\oam\\server\\lib\\upgrade\\ps1-policy directory.
OAM_PS1_CONFIG_FILE_LOC	This property refers to the Oracle Access Manager 11.1.1.x.x configuration files available in the following location: On UNIX, it is located in the $<DOMAIN_HOME>/config/fmwconfig/oam-config.xml directory. On Windows, it is located in the <DOMAIN_HOME>\\config\\fmwconfig\\oam-config.xml directory.
OAM_PS1_POLICY_FILE_TEMP	This property refers to the absolute path to the temporary policy XML. This temporary XML will be used for policy transformation. Specify the temporary location of the XML file. For example: On UNIX, specify the following path: OAM_PS1_POLICY_FILE_TEMP=<UPGRADE_ATRIFACTS_DIR>/oam-policy-ps1_temp.xml On Windows, specify the following path: OAM_PS1_POLICY_FILE_TEMP=<UPGRADE_ATRIFACTS_DIR>\\oam-policy-ps1_temp.xml
OAM_R2_POLICY_JARS	Upgrade frameworks loads version specific jars for exporting and importing data. This property refers to the Access Manager 11.1.2.2.0 policy jars available at the following location: On UNIX, it is located in the $<ORACLE_HOME>/oam/server/lib/upgrade/ps2-policy directory. On Windows, it is located in the <ORACLE_HOME>\\oam\\server\\lib\\upgrade\\ps2-policy directory.
OAM_R2_CONFIG_FILE_LOC	This property refers to the Access Manager 11.1.2.2.0 configuration files available at the following location: On UNIX, it is located in the $<ORACLE_HOME>/oam/server/config/oam-config.xml directory. On Windows, it is located in the <ORACLE_HOME>\\oam\\server\\config\\oam-config.xml directory.

Table 9–3 (Cont.) Property Description

Properties	Description
OAM_SOURCE_VERSION	The Oracle Access Manager source version is 11.1.1.x.x.
OAM_TARGET_VERSION	The Access Manager target version is 11.1.2.0.0.

Note: The variables listed in Table 9–3 are not environment variables. These variables must be defined in the oam_upgrade.properties file.

When you specify paths to any files in the oam_upgrade.properties file, make sure it is in the format specified in the following example:

- On UNIX: /directory_1/directory_2/file
- On Windows: \\directory_1\\directory_2\\file

Sample Output of exportAccessData

```
wls:/offline> exportAccessData("<ORACLE_HOME>/oam/server/wlst/scripts/sample_
properties/oam_upgrade.properties")
Jul 7, 2012 1:37:30 AM oracle.security.access.upgrade.WLSTExecutor executeCommand
INFO: EXPORT_DATA_COMMAND
Jul 7, 2012 1:37:30 AM oracle.security.access.upgrade.util.WLSTExportDataUtil
executeCommand
INFO: OAAM PRODUCT
Jul 7, 2012 1:37:30 AM oracle.security.access.upgrade.util.WLSTExportDataUtil
executeCommand
INFO: OAM PRODUCT
Jul 7, 2012 1:37:30 AM oracle.security.access.upgrade.util.WLSTExportDataUtil
executeCommand
INFO: oamPlugin.getName() =
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory
Jul 7, 2012 1:37:30 AM oracle.security.am.upgrade.plugin.util.UpgradeUtil
exportConfiguration
INFO: Copying configuration file....
oracle.security.am.upgrade.plugin.upgradehelper.OAMVersionSpecificClassLoader@1e33
0f43
[EL Info]: 2012-07-07 01:37:32.849--ServerSession(503497062)--EclipseLink,
version: Eclipse Persistence Services - 1.1.0.r3634
[EL Info]: 2012-07-07 01:37:35.212--ServerSession(503497062)--file:$ORACLE_
HOME/oam/server/lib/upgrade/ps1-policy/oes-d8/jps-internal.jar-JpsDBDataManager
login successful
Jul 7, 2012 1:37:39 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:37:39.026/135.466 Oracle Coherence 3.5.3/465p2 <Info>
(thread=Main Thread, member=n/a): Loaded operational configuration from resource
"jar:file:$ORACLE_
HOME/oam/server/lib/upgrade/ps1-policy/coherence.jar!/tangosol-coherence.xml"
Jul 7, 2012 1:37:39 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:37:39.035/135.474 Oracle Coherence 3.5.3/465p2 <Info>
(thread=Main Thread, member=n/a): Loaded operational overrides from resource
"jar:file:$ORACLE_
HOME/oam/server/lib/upgrade/ps1-policy/coherence.jar!/tangosol-coherence-override-
dev.xml"
...................
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:37:47 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:37:47 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
```

```
Jul 7, 2012 1:37:47 AM
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory exportData
INFO: Extraction Done!!
Jul 7, 2012 1:37:47 AM oracle.security.am.upgrade.plugin.util.UpgradeCommonUtil
removeDirectory
INFO: Deletion of Directory: true path: $OAM_ARTIFACTS_DIRECTORTY/temp.zip
Jul 7, 2012 1:37:47 AM
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory exportData
INFO: Export completed successfully!
```

9.13 Importing Access Data

It is necessary to import the extracted Oracle Access Manager 11.1.1.x.x data to the Access Manager 11.1.2 schema. The Oracle Access Manager 11.1.1.x.x domain configuration is also merged with the Access Manager 11.1.2 configuration.

> **Note:** Make sure to shutdown all WebLogic Server processes (administration server, Oracle Access Manager managed server, and node manager) before executing these import commands.

To import Oracle Access Manager 11.1.1.x.x configuration data into Access Manager 11.1.2.2.0, complete the following steps:

On UNIX:

1. Move from your present working directory to the `<MW_HOME>/<Oracle_IDM1>/common/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/<Oracle_IDM1>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. At the WLST prompt, run the following script:

   ```
   importAccessData("<UPGRADE_PROPERTIES_FILE>")
   ```

   For example:

   ```
   importAccessData("<ORACLE_HOME>/oam/server/wlst/scripts/sample_
   properties/oam_upgrade.properties")
   ```

   See Table 9–3 for sample properties and description.

4. Exit the WLST console using the `exit()` command.

On Windows:

1. Move from your present working directory to the `<MW_HOME>\<Oracle_IDM1>\common\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\<Oracle_IDM1>\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. At the WLST prompt, run the following script:

```
importAccessData("<UPGRADE_PROPERTIES_FILE>")
```

For example:

```
importAccessData("<ORACLE_HOME>\\oam\\server\\wlst\\scripts\\sample_
properties\\oam_upgrade.properties")
```

See Table 9–3 for sample properties and description.

4. Exit the WLST console using the `exit()` command.

Table 9–4 describes the parameters you need to specify on the command line:

Table 9–4 Parameters for Importing Data

Parameter	Description
`properties_location`	Specify the path to the `oam_upgrade.properties` file in the Oracle Access Manager 11.1.1.x.x installation. The following example shows the complete path: On UNIX, it is located in the `IDM_HOME/oam/server/wlst/scripts/sample_properties/oam_upgrade.properties` directory. On Windows, it is located in the `IDM_HOME\oam\server\wlst\scripts\sample_properties\oam_upgrade.properties` directory.

Sample Output of importAccessData

```
wls:/offline> importAccessData("<ORACLE_HOME>/oam/server/wlst/scripts/sample_
properties/oam_upgrade.properties")
LOGGER intialised java.util.logging.Logger@1e26e4b1
Jul 7, 2012 1:38:25 AM oracle.security.access.upgrade.WLSTExecutor executeCommand
INFO: IMPORT_DATA_COMMAND
Jul 7, 2012 1:38:25 AM oracle.security.access.upgrade.util.WLSTImportDataUtil
executeCommand
INFO: OAAM PRODUCT IMPORT DATA
Jul 7, 2012 1:38:25 AM oracle.security.access.upgrade.util.WLSTImportDataUtil
executeCommand
INFO: OAM PRODUCT
Jul 7, 2012 1:38:25 AM oracle.security.access.upgrade.util.WLSTImportDataUtil
executeCommand
INFO: oamPlugin.getName() =
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory
Jul 7, 2012 1:38:27 AM
oracle.security.am.common.policy.admin.provider.xml.XMLStore <init>
INFO: Loading policy store file: $OAM_ARTIFACTS_DIRECTORTY/oam-policy.xml.
Jul 7, 2012 1:38:30 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:38:30.069/17.816 Oracle Coherence 3.7.1.1 <Info> (thread=Main
Thread, member=n/a): Loaded operational configuration from "jar:file:$MIDDLEWARE_
HOMEoracle_common/modules/oracle.coherence/coherence.jar!/tangosol-coherence.xml"
Jul 7, 2012 1:38:30 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:38:30.103/17.850 Oracle Coherence 3.7.1.1 <Info> (thread=Main
Thread, member=n/a): Loaded operational overrides from "jar:file:$MIDDLEWARE_
HOMEoracle_
common/modules/oracle.coherence/coherence.jar!/tangosol-coherence-override-dev.xml
"
Jul 7, 2012 1:38:30 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:38:30.107/17.854 Oracle Coherence 3.7.1.1 <Info> (thread=Main
Thread, member=n/a): Loaded operational overrides from "jar:file:$ORACLE_
HOME/oam/server/lib/upgrade/ps2-policy/mapstore-coherence.jar!/tangosol-coherence-
override.xml"
.....
```

```
Jul 7, 2012 1:38:36 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:38:36 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:38:36 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:38:38 AM
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory importData
INFO: Import completed successfully!!
```

Note: When you execute the `importAccessData()` command, the output might include additional text after the line `INFO: Import completed successfully!!`. The additional text has no impact on the result and can be ignored.

9.14 Copying Modified System mbean Configurations

After updating the Access Manager binaries to 11.1.2.2.0 you must copy the modified system or domain mbean configurations from the *OAM_ORACLE_HOME* to the *DOMAIN_HOME*.

On UNIX:

1. Move from your present working directory to the `<MW_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME><Oracle_IDM1>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. At the WLST prompt, run the following script:

   ```
   copyMbeanXmlFiles('DOMAIN_HOME','OAM_ORACLE_HOME')
   ```

   For example:

   ```
   copyMbeanXmlFiles('/Oracle/Middleware/user_projects/domains/base_
   domain','/Oracle/Middleware/Oracle_IDM1')
   ```

4. Exit the WLST console using the `exit()` command.

On Windows:

1. Move from your present working directory to the `<MW_HOME>\common\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\<Oracle_IDM1>\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. At the WLST prompt, run the following script:

   ```
   copyMbeanXmlFiles ('<domain_name>',' 'Oracle_IDM')
   ```

   For example:

   ```
   copyMbeanXmlFiles('C:\\Oracle\\Middleware\\user_projects\domains\\base_
   domain','C:\\Oracle\\Middleware\\Oracle_IDM1')
   ```

4. Exit the WLST console using the `exit()` command.

9.15 Starting the Administration Server and Access Manager Managed Servers

> **Note:** When you start the Administration Server and the Managed Servers, the Access Manager Administration console application and the Access Manager Managed server application may start with a number of errors and exceptions. This is expected and can be ignored. These issues are resolved by the subsequent redeployment process.

The `redeploy` command is an online WLST command. Therefore, you must start the Oracle Access Management Access Manager Administration and Managed Servers before running the `redeploy` command.

For information about starting the Administration Server and Access Manager Managed servers, see "Starting the Servers" on page 2-12.

9.16 Redeploying Oracle Access Management Access Manager Servers and Shared Libraries

You must redeploy Oracle Access Management Access Manager for the following reasons:

- To uptake new shared libraries that Access Manager servers are dependent on.
- To uptake newer versions of Access Manager Administration and Managed Server applications.

To redeploy Access Manager server applications and shared Access Manager libraries, complete the following steps:

1. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location *$MW_HOME*/*ORACLE_HOME*/`common/bin`:

   On UNIX: `./wlst.sh`

   On Windows: `wlst.cmd`

2. Connect to the Administration Server using the following command:

   ```
   connect('<weblogic_username>','<weblogic_password>','<weblogic_
   host>:<port>')
   ```

3. Run the following command to redeploy the applications and shared libraries:

   ```
   redeployOAM("ORACLE_HOME","ORACLE_COMMON_HOME",adminTarget="Admin_
   server_name",serverTarget="oam_server")
   ```

   > **Note:** If you are upgrading Oracle Access Manager high availability environments, speciy the `oam_cluster` for the argument `serverTarget` while running `redeployOAM` command.

   Table 9–5 describes the parameters you need to specify on the command line:

Table 9–5 Parameters to be Specified When Running redeployOAM Command

Parameter	Description
ORACLE_HOME	Specify the absolute path to the Oracle Home. For example: On UNIX, it is located at `Oracle/Middlewar`e directory. On Windows, it is located at `Oracle\Middleware` directory.
ORACLE_COMMON_HOME	Specify the absolute path to the Oracle common home. For example: On UNIX, it is located in the `Oracle/Middleware/Common_home` directory. On Windows, it is located in the `Oracle\Middleware\Common_home` directory.
`adminTarget`	Specify the Administration Server name you had specified while configuring Access Manager.
`serverTarget`	Specify the name of the Access Manager Server you had specified while configuring Access Manager Server.

For example:

```
redeployOAM("/scratch/Oracle/Middleware/Oracle_
IDM1","/scratch/Oracle/Middleware/oracle_
common",adminTarget="AdminServer",serverTarget="OAM_SERVER")
```

Note:

- You might see the following exception after the Access Manager server deployment. This is because `tmp` and `stage` directories still exist. You can ignore the errors:

```
HTTP:101216]Servlet: "AMInitServlet" failed to preload on
startup in Web application: "oam".
java.lang.ExceptionInInitializerError
at java.lang.J9VMInternals.initialize(J9VMInternals.java:222)
at
oracle.security.am.engines.sso.adapter.AbstractSessionAdapterIm
pl.checkAndInit(AbstractSessionAdapterImpl.java:97)
at
oracle.security.am.engines.sso.adapter.AbstractSessionAdapterIm
pl.<init>(AbstractSessionAdapterImpl.java:75)
at
oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapt
erImpl.<init>(MultipleUserSessionAdapterImpl.java:56
at
oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapt
erImpl.<clinit>(MultipleUserSessionAdapterImpl.java:45)
at java.lang.J9VMInternals.initializeImpl(Native Method)
at java.lang.J9VMInternals.initialize(J9VMInternals.java:200)
at
oracle.security.am.engines.sso.adapter.SessionManagementAdapter
Factory.getAdapter(SessionManagementAdapterFactory.java:46
Caused by:
oracle.security.am.common.utilities.exception.AmRuntimeExceptio
n:OAM Server Key initialization failed
Caused by: javax.crypto.BadPaddingException: Given final block
not properly padded
```

- When you execute the `redeployOAM` command, the following warning may be displayed:

```
"********************** Performing OAM Admin server
deployment and Data Migration. This operation will take some
time. Please wait until it completes.******"
```

  Note that redeployment takes approximately 30 minutes to complete due to policy migration. In addition, note that the time for completion of redeployment also depends on the amount of data present in the Oracle Access Manager system that is being upgraded.

4. Exit the WLST console using the `exit()` command.

The deployment may fail if the SDP library is already installed as a part of the SOA or OIM deployments. For recovery procedure, see Section 9.22.2, "Exception While Deploying Application".

Note: .

After redeploying Oracle Access Management Access Manager, you must verify that the following libraries and applications are deployed to Access Manager cluster (`OAM_CLUSTER`):

Libraries

- `oracle.oaam.libs (11.1.2.0.0)`
- `oracle.sdp.client (11.1.1)`
- `coherence (3.7.1.1)`
- `oracle.idm.ids.config.ui (11.1.2,11.1.2)`
- `oracle.idm.ipf (11.1.2,11.1.2)`

Applications

- `oamsso_logout (11.1.2.0.0)`
- `oam_server (11.1.2.0.0)`

9.17 Stopping the Administration Server and Access Manager Managed Servers

To stop the servers, see Section 9.3, "Shutting Down Administration Server and Managed Servers".

9.18 Deleting Folders

This step is required to uptake new version of the Access Manager Managed Server. The `redeploy` command does not delete the `tmp` directories.

In order to deploy Oracle Access Manager 11.1.1.x.x server content and applications to Access Manager 11.1.2.2.0, you must delete all folders in the following location:

On UNIX:

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAM_MANAGED_SERVER_
NAME>
```

On Windows:

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAM_MANAGED_SERVER_
NAME>
```

9.19 Upgrading System Configuration

After you upgrade to Oracle Access Manager binaries to 11.1.2.2.0, you must run the `upgradeConfig()` utility on the machine that hosts Administration Server, to upgrade the system configuration of Oracle Access Manager to 11.1.2.2.0. Before you run the `upgradeConfig()` utility, make sure that the Administration Server and the Managed Servers are stopped.

To upgrade the system configuration of Oracle Access Manager, do the following:

1. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location *`$ORACLE_HOME`*`/common/bin`:

On UNIX: `./wlst.sh`

On Windows: `wlst.cmd`

2. Run the following command in offline mode:

```
upgradeConfig("domain_home", "sysdbaUser", "sysdbaPwd",
"oamSchemaOwner", "oamdbJdbcUrl")
```

In this command,

- *domain_home* is the absolute path to the Access Manager WebLogic domain.
- *sysdbauser* is the database username having `sysdba` privileges.
- *sysdbapwd* is the password of the database user having `sysdba` privileges.
- *oamSchemaOwner* is the database username for OAM schema.
- *oamdbjdbcUrl* is the JDBC URL to connect to the Access Manager database. The JDBC URL must be in specified in the format `"jdbc:oracle:thin:@<server_host>:<server_port>/<service_name>"`.

For example:

On UNIX:

```
upgradeConfig("/Oracle/Middleware/user_projects/domains/base_domain",
"sys", "pwd", "PREFIX_OAM", "jdbc:oracle:thin:@localhost:1521/orcl")
```

On Windows:

```
upgradeConfig("C:\\Oracle\\Middleware\\user_projects\\domains\\base_
domain", "sys", "pwd", "PREFIX_OAM",
"jdbc:oracle:thin:@localhost:1521/orcl")
```

9.20 Starting the Administration Server and Access Manager Managed Servers

To start the servers, see Section 9.15, "Starting the Administration Server and Access Manager Managed Servers".

9.21 Verifying the Upgrade

Use the following URL in a web browser to verify that Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0) is running:

```
http(s)://<oam_admin_server_host>:<oam_admin_server_port>/oamconsole
```

Note: This note is applicable only to users who currently have Oracle Identity Manager and Oracle Access Manager components integrated in 11*g* R1 (11.1.1.5.1) or earlier versions, and are upgrading both Oracle Identity Manager and Access Manager to 11*g* R2 (11.1.2).

After upgrading the components to 11*g* Release 2 (11.1.2.2.0), see "Using the idmConfigTool Command" in the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

9.22 Troubleshooting

This sections describes some of the common issues that you might encounter during the upgrade process, and their workarounds.

> **Note:** For information about the issues that you might encounter during the upgrade process, and their workarounds, see *Oracle Fusion Middleware Release Notes*.

This section contains the following topics:

- Exception While Running ImportAccessData Command
- Exception While Deploying Application
- Exception While Restarting Administration Server
- Exception While Restarting Managed Server
- Component Version Shows 11.1.1.5.0 After Upgrade

9.22.1 Exception While Running ImportAccessData Command

If you get a `class not found` exception, it is because you have not exited from the WLST console after running the `exportAccessData` command.

Exit the WLST console using the `exit()` command.

9.22.2 Exception While Deploying Application

- If you get the following exception when you deploy `sdpclient.jar` application, then the SDP library is already installed.

```
<Month <Date>, <Year> <Time> <Time ZOne> <Info> <J2EE Deployment SPI>
<BEA-260121> <Initiating deploy operation for application,
oracle.sdp.client#11.1.1@11.1.1 [archive: <ORACLE_
HOME>/communications/modules/oracle.sdp.client_11.1.1/sdpclient.jar], to oam_
server1 .>
weblogic.management.ManagementException: [Deployer:149007]New source location,
'<ORACLE_HOME>/communications/modules/oracle.sdp.client_11.1.1/sdpclient.jar',
cannot be deployed to configured application, 'oracle.sdp.client
[LibSpecVersion=11.1.1,LibImplVersion=11.1.1]'. The application source is at
'<ORACLE_SOA_HOME>/communications/modules/oracle.sdp.client_
11.1.1/sdpclient.jar'. Changing the source location is not allowed for a
previously attempted deployment. Try deploying without specifying the
source.Failed to deploy the application with status failed
Current Status of your Deployment:
Deployment command type: deploy
Deployment State : failed
Deployment Message : weblogic.management.ManagementException:
[Deployer:149007]New source location, '<ORACLE_
HOME>/communications/modules/oracle.sdp.client_11.1.1/sdpclient.jar', cannot be
deployed to configured application, 'oracle.sdp.client
[LibSpecVersion=11.1.1,LibImplVersion=11.1.1]'. The application source is at
'<ORACLE_SOA_HOME>/communications/modules/oracle.sdp.client_
11.1.1/sdpclient.jar'. Changing the source location is not allowed for a
previously attempted deployment. Try deploying without specifying the source.
Error occured while performing deploy : Target exception thrown while deploying
application: Error occured while performing deploy : Deployment Failed. : Error
occured while performing deploy : Deployment Failed.
```

```
Use dumpStack() to view the full stacktrace
Deploying application from <ORACLE_HOME>/oam/server/apps/oam-admin.ear to
targets AdminServer (upload=false) ...
```

Complete the following steps to recover:

1. Log into the WebLogic console.
2. Check for the following library:

   oracle.sdp.client(11.1.1,11.1.1)
3. Target this library to `oam_server1`
4. Run the following command:

   ```
   deployOAMServer("<ORACLE_
   HOME>",adminTarget="AdminServer",serverTarget="oam_server1")
   ```

- If you get the following error after the Access Manager server deployment, it is because the `tmp` and `stage` directories still exist in your environment.

  Ignore it:

```
[HTTP:101216]Servlet: "AMInitServlet" failed to preload on startup in Web
application: "oam".
java.lang.ExceptionInInitializerError
at java.lang.J9VMInternals.initialize(J9VMInternals.java:222)
at
oracle.security.am.engines.sso.adapter.AbstractSessionAdapterImpl.checkAndInit(
AbstractSessionAdapterImpl.java:97)
at
oracle.security.am.engines.sso.adapter.AbstractSessionAdapterImpl.<init>(Abstra
ctSessionAdapterImpl.java:75)
at
oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapterImpl.<init>(Mu
ltipleUserSessionAdapterImpl.java:56)
at
oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapterImpl.<clinit>(
MultipleUserSessionAdapterImpl.java:45)
at java.lang.J9VMInternals.initializeImpl(Native Method)
at java.lang.J9VMInternals.initialize(J9VMInternals.java:200)
at
oracle.security.am.engines.sso.adapter.SessionManagementAdapterFactory.getAdapt
er(SessionManagementAdapterFactory.java:46)
```

9.22.3 Exception While Restarting Administration Server

If you get the following error, the 11.1.2.2.0 Repository Creation Utility is not new and has data.

```
oracle.security.am.common.policy.admin.impl.PolicyValidationException:
OAMSSA-06045: An object of this type named "HTTP" already exists.
at
oracle.security.am.common.policy.admin.impl.ResourceTypeManagerImpl.isValidWrite(R
esourceTypeManagerImpl.java:482)
at
oracle.security.am.common.policy.admin.impl.ResourceTypeManagerImpl.createResource
Type(ResourceTypeManagerImpl.java:165)
at
oracle.security.am.common.policy.tools.OAMPolicyStoreBootstrap.createResourceType(
OAMPolicyStoreBootstrap.java:554)
at
```

```
oracle.security.am.common.policy.tools.OAMPolicyStoreBootstrap.addOAMObjs(OAMPolic
yStoreBootstrap.java:328)
at
oracle.security.am.common.policy.tools.OAMPolicyStoreBootstrap.addPolicyObjects(OA
MPolicyStoreBootstrap.java:280)
at
oracle.security.am.common.policy.tools.OAMPolicyStoreBootstrap.bootstrap(OAMPolicy
StoreBootstrap.java:233)
at oracle.security.am.install.OAMInstaller.bootstrapOES(OAMInstaller.java:1064)
at oracle.security.am.install.OAMInstaller.bootstrapPolicy(OAMInstaller.java:1423)
at oracle.security.am.install.OAMInstaller.upgradePolicy(OAMInstaller.java:1513)
```

Check if a new Repository Creation Utility schema is created for Access Manager. Also check if the domain has been updated to use the new 11.1.2.2.0 Repository Creation Utility.

9.22.4 Exception While Restarting Managed Server

If you get the following error, the `tmp` and `stage` folders still exists:

```
Caused by:
com.bea.security.ParameterException: Invalid configuration: cannot locate class:
com.bea.security.ssal.micro.MicroSecurityServiceManagerWrapper
at
com.bea.security.impl.SecurityRuntimeImpl.getNewInstance(SecurityRuntimeImpl.java:
263)
at
com.bea.security.impl.SecurityRuntimeImpl.initialize(SecurityRuntimeImpl.java:313)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:
25)
at java.lang.reflect.Method.invoke(Method.java:597)
at com.bea.security.SecurityRuntime.initialize(SecurityRuntime.java:140)
at com.bea.security.impl.MicroSMImpl.getInstance(MicroSMImpl.java:167)
```

This error is resolved once you remove the `tmp` and `stage` folders, as instructed in Section 9.18, "Deleting Folders".

9.22.5 Component Version Shows 11.1.1.5.0 After Upgrade

If you upgraded Oracle Access Manager 11*g* Release 1 (11.1.1.5.0) to 11.1.2.2.0, the component versions of the packages `oracle.dogwood.top` and `oracle.oam.server` still show 11.1.1.5.0.

The resolve this, you must run the domain updater utility (`com.oracle.cie.domain-update_1.0.0.0.jar`). This step updates the `domain-info.xml`.

To upgrade the necessary Oracle Access Manager packages to 11.1.2.2.0, complete the following steps:

1. Go to the directory *$ORACLE_HOME*`/oaam/upgrade`. The domain updater utility `com.oracle.cie.domain-update_1.0.0.0.jar` file is located in this directory.
2. Upgrade the package `oracle.dogwood.top` 11.1.1.5.0 to 11.1.2.2.0 by running the following command:

   ```
   java -cp $MW_
   HOME/utils/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
   ```

```
_1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <DOMAIN_HOME>
oracle.dogwood.top:11.1.1.5.0,:11.1.2.2.0
```

For example:

```
java -cp
/scratch/Oracle/Middleware/utils/config/10.3/config-launch.jar:./com.or
acle.cie.domain-update_1.0.0.0.jar
com.oracle.cie.external.domain.DomainUpdater
/scratch/Oracle/Middleware/user_projects/domains/OAMDomain
oracle.dogwood.top:11.1.1.5.0,:11.1.2.2.0
```

3. Upgrade the package `oracle.oam.server` 11.1.1.5.0 to 11.1.2.2.0 by running the following command:

```
java -cp $MW_
HOME/utils/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
_1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <DOMAIN_HOME>
oracle.oam.server:11.1.1.5.0,:11.1.2.2.0
```

For example:

```
java -cp
/scratch/Oracle/Middleware/utils/config/10.3/config-launch.jar:./com.or
acle.cie.domain-update_1.0.0.0.jar
com.oracle.cie.external.domain.DomainUpdater
/scratch/Oracle/Middleware/user_projects/domains/OAMDomain
oracle.oam.server:11.1.1.5.0,:11.1.2.2.0
```

10

Upgrading Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.x.x) Environments

This chapter describes how to upgrade your existing Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0) and 11*g* Release 1 (11.1.1.7.0) environments to Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

Note: For information about upgrading Oracle Adaptive Access Manager on IBM WebSphere, see "Upgrading Oracle Adaptive Access Manager on IBM WebSphere" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

Note: This chapter refers to Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.0) and 11g Release 1 (11.1.1.7.0) environments as 11.1.1.x.x.

This chapter includes the following sections:

- Upgrade Roadmap for Oracle Adaptive Access Manager
- Reviewing System Requirements and Certification
- Shutting Down Administration Server and Managed Servers
- Backing Up Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x)
- Optional: Upgrading Oracle WebLogic Server
- Upgrading Oracle Adaptive Access Manager 11g Release 2 (11.1.2.2.0)
- Upgrading OAAM, MDS, IAU, and OPSS Schemas
- Extending Oracle Adaptive Access Manager 11.1.1.x.x Component Domains with OPSS Template
- Upgrading Oracle Platform Security Services
- Configuring OPSS Security Store
- Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers
- Redeploying the Applications
- Deleting Folders
- Restarting the Servers

- Verifying the Upgrade

10.1 Upgrade Roadmap for Oracle Adaptive Access Manager

Note: If you do not follow the exact sequence provided in this task table, your Oracle Adaptive Access Manager upgrade may not be successful.

Table 10–1 lists the steps to upgrade Oracle Adaptive Access Manager.

Table 10–1 Upgrade Flow

	Task	For More Information
1	Review system requirements and certifications.	See, Reviewing System Requirements and Certification
2	Shut down all servers. This includes both Administration Server and Managed Servers.	See, Shutting Down Administration Server and Managed Servers
3	Back up your environment.	See, Backing Up Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x)
4	Optional - Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6.	See, Optional: Upgrading Oracle WebLogic Server
5	Upgrade 11.1.1.x.x Oracle Home to 11.1.2.2.0.	See, Upgrading Oracle Adaptive Access Manager 11g Release 2 (11.1.2.2.0)
6	Upgrade the OAAM, MDS, IAU, and OPSS Schemas using Patch Set Assistant.	See, Upgrading OAAM, MDS, IAU, and OPSS Schemas
7	Extend your Oracle Adaptive Access Manager 11.1.1.x.x domain with the OPSS template.	See, Extending Oracle Adaptive Access Manager 11.1.1.x.x Component Domains with OPSS Template
8	Upgrade Oracle Platform Security Services, if required.	See, Upgrading Oracle Platform Security Services
9	Run the `configuresecuritystore.py` script to configure policy stores.	See, Configuring OPSS Security Store
10	Start the Administration and Managed Servers.	See, Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers
11	Redeploy the applications on Oracle Adaptive Access Manager 11.1.2.2.0 Servers.	See, Redeploying the Applications
12	Delete the `tmp` and `stage` folders.	See, Deleting Folders
13	Restart the servers.	See, Restarting the Servers
14	Verify the Oracle Adaptive Access Manager upgrade.	See, Verifying the Upgrade

10.2 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements

for the products you are installing or upgrading. For more information see Section 2.1, "Reviewing System Requirements and Certification".

10.3 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the WebLogic Administration Server and the Oracle Adaptive Access Manager Managed Servers.

For more information about stopping the WebLogic Administration Server and the Managed Servers, see Section 2.8, "Stopping the Servers".

10.4 Backing Up Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x)

You must back up your Oracle Adaptive Access Manager 11.1.1.x.x environment before you upgrade to Oracle Adaptive Access Manager 11.1.2.2.0.

After stopping the servers, you must back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Adaptive Access Manager schemas
- IAU schema, if it is part of any of your Oracle Adaptive Access Manager 11.1.1.x.x schemas
- MDS schemas

10.5 Optional: Upgrading Oracle WebLogic Server

Note: Upgrading Oracle WebLogic Server is not mandatory. However, Oracle recommends that you upgrade Oracle WebLogic Server to 10.3.6.

You can upgrade WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6 by using the WebLogic 10.3.6 Upgrade Installer. For information about upgrading Oracle WebLogic Server, see Section 2.3, "Upgrading to Oracle WebLogic Server 10.3.6".

10.6 Upgrading Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.2.0)

To upgrade Oracle Adaptive Access Manager, you must use the Oracle Identity and Access Management 11.1.2.2.0 Installer. During the procedure, point the Middleware Home to your existing 11.1.1.x.x Middleware Home. Your Oracle Home is upgraded from 11.1.1.x.x to 11.1.2.2.0.

For information about upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x), see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

10.7 Upgrading OAAM, MDS, IAU, and OPSS Schemas

You must upgrade the following schemas using Patch Set Assistant:

- OAAM schema
- MDS schema
- OPSS schema

> **Note:** If OPSS schema is not part of the source, a new OPSS schema must first be created using 11.1.2.2.0 RCU and only then can it be upgraded. You must create Oracle Platform Security Services (OPSS) schema because Oracle Adaptive Access Manager upgrade process involves OPSS schema policy store changes. Keys, roles, permissions, and other artifacts used by the applications must migrate to the policy store.
>
> Run Repository Creation utility (RCU) to create the OPSS schema. For more information, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

- IAU schema (You must upgrade Audit schema (IAU) only if it is part of your 11.1.1.x.x schemas.

> **Note:** When upgrading schemas using Patch Set Assistant, you must select **OAAM** or **OAAM_PARTN** as appropriate, and provide details on all screens to complete the upgrade.

For information about upgrading schemas using Patch Set Assistant, see Section 2.6, "Upgrading Schemas Using Patch Set Assistant".

10.8 Extending Oracle Adaptive Access Manager 11.1.1.x.x Component Domains with OPSS Template

Oracle Adaptive Access Manager 11.1.2.2.0 uses the database to store policies. This requires extending the 11.1.1.x.x Oracle Adaptive Access Manager domain to include the OPSS data source.

To do so, complete the following steps:

1. Run the following command to launch the Oracle Fusion Middleware configuration wizard:

   On UNIX:

   `./config.sh`

   It is located in the `<MW_HOME>/<Oracle_IDM1>/common/bin` directory.

   On Windows:

   `config.cmd`

   It is located in the `<MW_HOME>\<Oracle_IDM1>\common\bin` directory.

2. On the **Welcome** screen, select the **Extend an existing WebLogic domain** option. Click **Next**.

3. On the **Select a WebLogic Domain Directory** screen, browse to the directory that contains the WebLogic domain in which you configured the components. Click **Next**. The **Select Extension Source** screen is displayed.
4. On the **Select Extension Source** screen, select the **Oracle Platform Security Service - 11.1.1.0 [Oracle_IDM1]** option. After selecting the domain configuration options, click **Next**.
5. The **Configure JDBC Data Sources** screen is displayed. Configure the opssDS data source, as required. After the test succeeds, the **Configure JDBC Component Schema** screen is displayed.
6. On the **Configure JDBC Component Schema** screen, select the **Oracle Platform Security Services** schema.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**.

   The **Test JDBC Component Schema** screen is displayed. After the test succeeds, the **Select Optional Configuration** screen is displayed.
7. On the **Select Optional Configuration** screen, you can configure Managed Servers, Clusters, and Machines and Deployments and Services. Do not select anything as you have already configured in your Oracle Identity and Access Management 11.1.1.x.x environment. Click **Next**.
8. On the **Configuration Summary** screen, review the domain configuration, and click **Extend** to start extending the domain.

Your existing Oracle Adaptive Access Manager domain is extended to support Oracle Platform Security Services (OPSS).

10.9 Upgrading Oracle Platform Security Services

> **Note:** The upgrade steps need to be performed only if OPSS has already been configured.

After you upgrade schemas, you must upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Adaptive Access Manager to 11.1.2.2.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see Section 2.7, "Upgrading Oracle Platform Security Services".

10.10 Configuring OPSS Security Store

> **Note:** You need to configure OPSS Security Store only if it was not configured during the previous installation. If it has already been configured, perform the steps to upgrade OPSS. For more information, see Section 10.9, "Upgrading Oracle Platform Security Services".

You must configure the database Security Store as it is the only security store type supported by Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0).

For more information on configuring Oracle Platform Security Services, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

10.11 Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers

Note: When you start the Administration Server and the Managed Servers, the Adaptive Access Manager Administration console application and the Access Manager Managed server application may start with a number of errors and exceptions. This is expected and can be ignored. These issues are resolved by the subsequent redeployment process.

The `redeploy` command is an online WLST command. Therefore, you must start the Oracle Adaptive Access Manager Administration and Managed Servers before running the `redeploy` command.

For information about starting the Administration Server and Oracle Adaptive Access Manager Managed servers, see "Starting the Servers" on page 2-12.

10.12 Redeploying the Applications

You must redeploy changes to the applications in the domain after upgrading Oracle Adaptive Access Manager to 11.1.2.2.0. Redeploy your 11.1.1.x.x application on the Oracle Adaptive Access Manager 11.1.2.2.0 servers.

You can redeploy the application using command line or using the WebLogic Administration console. Complete the following steps described in one of the following sections to redeploy applications:

- Redeploying Applications Using Command Line
- Redeploying Applications Using WebLogic Administration Console

Redeploying Applications Using Command Line

To redeploy applications on Oracle Adaptive Access Manager 11.1.2.2.0 servers using command line, do the following:

1. Run the following command from the location *`IAM_HOME`*`/common/bin` to launch the WebLogic Scripting Tool (WLST):

   On UNIX: `./wlst.sh`

   On Windows: `wlst.cmd`

2. Connect to the Administration Server using the following command:

   `connect('`*`weblogic-username`*`','`*`weblogic-password`*`','`*`weblogic-url`*`')`

   For example:

   `connect('wlsuser','wlspassword','localhost:7001')`

3. Run the following command to undeploy OAAM:

   `undeploy('oaam_admin')`

```
undeploy('oaam_server')

undeploy('oracle.oaam.extensions')
```

> **Note:** If you have Oracle Adaptive Access Manager Offline Server in your setup, run the `undeploy()` command to undeploy `'oaam_offline'` too.

For more information about using the `undeploy` command, see "undeploy" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

4. Deploy the `oaam.extension` library application by running the following command:

```
deploy('oracle.oaam.extensions','$IAM_HOME/oaam/oaam_
extensions/generic/oracle.oaam.extensions.war','oaam_admin_
server1,oaam_server_server1','nostage',libraryModule='true')
```

> **Note:** If you have Oracle Adaptive Access Manager Offline Server in your setup, add `oaam_offline_server1` to the list of targets while deploying `oaam.extension` library.

For more information about using the `deploy` command, see "deploy" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

5. Deploy the OAAM applications by running the following commands:

```
deploy('oaam_admin','$IAM_HOME/oaam/oaam_admin/ear/oaam_
admin.ear','oaam_admin_server1','nostage')

deploy('oaam_server','$IAM_HOME/oaam/oaam_server/ear/oaam_
server.ear','oaam_server_server1','nostage')
```

The target servers for each deployments are as follows:

- `oaam_admin` - Target: `oaam_admin_server1`
- `oaam_server` - Target: `oaam_server_server1`

> **Note:** If you have Oracle Adaptive Access Manager Offline Server in your setup, deploy `'oaam_offline'` to the target `'oaam_offline_server1'` by running the `deploy()` command.

For more information about using the `deploy` command, see "deploy" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

6. Optional: If you had deployed the OAAM shared library, run the following command to redeploy it:

```
redeploy('oracle.oaam.libs')
```

7. Exit the WLST console using the `exit()` command.

Redeploying Applications Using WebLogic Administration Console

To redeploy applications on Oracle Adaptive Access Manager 11.1.2.2.0 servers using WebLogic Administration console, do the following:

1. Log in to the WebLogic Administration console using the following URL:

http://*admin_host*:*admin_port*/console:

2. Go to the **Deployments** tab.
3. Select oaam_admin, oaam_server and oracle.oaam.extensions from **Deployments** and click **Delete**.
4. Click **Install**, and specify the path for:
   - oracle.oaam.extensions and deploy it to oaam_server_server1 and other Oracle Adaptive Access Manager managed servers.

     Note: Ensure that oracle.oaam.extensions is redeployed before other applications.

   - oaam_admin.ear and deploy it to oaam_admin_server1 and other Oracle Adaptive Access Manager managed servers.
   - oaam_server.ear and deploy it to oaam_server_server1 and other Oracle Adaptive Access Manager managed servers.

   The target servers for each redeployment are as follows:

   - oracle.oaam.extensions - Targets: oaam_server_server1, oaam_admin_server1
   - oaam_admin - Target: oaam_admin_server1
   - oaam_server - Target: oaam_server_server1

10.13 Deleting Folders

To deploy Oracle Adaptive Access Manager 11.1.1.x.x server content and applications in Oracle Adaptive Access Manager 11.1.2.2.0, you must delete all content of folders in the following locations:

On UNIX:

Deleting tmp:

<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_ADMIN_SERVER_NAME>/tmp

<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_MANAGED_SERVER_NAME>/tmp

<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_OFFLINE_SERVER_NAME>/tmp

Deleting stage:

<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_ADMIN_SERVER_NAME>/stage

<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_MANAGED_SERVER_NAME>/stage

<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_OFFLINE_SERVER_NAME>/stage

On Windows:

Deleting tmp:

<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_ADMIN_SERVER_NAME>\tmp

<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_MANAGED_SERVER_NAME>\tmp

<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_OFFLINE_SERVER_NAME>\tmp

Deleting stage:

<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_ADMIN_SERVER_NAME>\stage

<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_MANAGED_SERVER_NAME>\stage

<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_OFFLINE_SERVER_NAME>\stage

10.14 Restarting the Servers

To restart the Administration Server or Managed Servers, you must stop the running Administration Server or Managed Servers first before starting them again.

To stop the servers, see Section 10.3, "Shutting Down Administration Server and Managed Servers".

To start the servers, see Section 10.11, "Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers".

Note: After all the upgrade steps are complete, check to make sure that the custom extensions (if any) are working correctly.

10.15 Verifying the Upgrade

Use the following URL in a web browser to verify that Oracle Adaptive Access Manager 11.1.2.2.0 is running:

http://<oaam_host>:<oaam_port>/oaam_admin

Assign the investigator role and verify to see the investigator UI.

11

Upgrading Oracle Identity Manager 11*g* Release 1 (11.1.1.x.x) Environments

This chapter describes how to upgrade your existing Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) and 11*g* Release 1 (11.1.1.7.0) environments to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

Note: For information about upgrading Oracle Identity Manager on IBM WebSphere, see "Upgrading Oracle Identity Manager on IBM WebSphere" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

Note: This chapter refers to Oracle Identity Manager 11g Release 1 (11.1.1.5.0) and 11g Release 1 (11.1.1.7.0) environments as 11.1.1.x.x.

This chapter includes the following sections:

- Section 11.1, "Upgrade Roadmap for Oracle Identity Manager"
- Section 11.2, "Pre-Upgrade"
- Section 11.3, "Upgrade Procedure"
- Section 11.4, "Post-Upgrade Steps"
- Section 11.5, "Troubleshooting"

Note: Oracle Identity Manager upgrade scripts from 11.1.1.x.x to 11.1.2.2.0 create application instances during the upgrade process. The application instances that are created will be based on the existing accounts and their data. For active accounts that have an IT Resource field on the process form, whose value is populated on the process form, corresponding application instances will be created for the specific Resource Object+ITResource combination.

11.1 Upgrade Roadmap for Oracle Identity Manager

The procedure for upgrading Oracle Identity Manager 11.1.1.x.x to 11.1.2.2.0 involves the following high-level steps:

1. **Pre-Upgrade Steps**: This step involves tasks like generating the pre-upgrade report, analyzing the report and performing the necessary pre-upgrade tasks

described in the report, shutting down the servers, backing up the 11.1.1.x.x environment and so on.

2. **Upgrading the Oracle Home and Database Schemas**: This step involves tasks like upgrading Oracle SOA Suite, upgrading 11.1.1.x.x Oracle Home to 11.1.2.2.0, creating Oracle Platform Security Services schema using Repository Creation Utility, upgrading Oracle Platform Security Services, configuring the security store, upgrading Oracle Identity Manager using Patch Set Assistant and so on.
3. **Upgrading the Oracle Identity Manager Middle Tier**: This step involves tasks like upgrading Oracle Identity Manager middle tier, starting the servers, patching the Oracle Identity Manager MDS metadata and so on.
4. **Upgrading Other Oracle Identity Manager Installed Components**: This step involves tasks like upgrading Oracle Identity Manager Design Console, Oracle Identity Manager Remote Manger, and configuring BI Publisher Reports.
5. **Post-Upgrade Steps**: This step involves the post-upgrade tasks like enabling Oracle Identity Manager - Oracle Access Manager integration, upgrading user UDF, customizing event handlers, upgrading SOA composites and so on.

Table 11–1 lists the steps to upgrade Oracle Identity Manager 11.1.1.x.x.

Note: If you do not follow the exact sequence provided in this task table, your Oracle Identity Manager upgrade may not be successful.

Table 11–1 Upgrade Flow

Sl No	Task	For More Information
	Pre-Upgrade Steps	
1	Review the changes in the features of Oracle Identity Manager 11.1.2.2.0.	See, Feature Comparison
2	Review system requirements and certifications.	See, Reviewing System Requirements and Certification
3	Generate the pre-upgrade report by running the `PreUpgradeReport` utility.	See, Generating and Analyzing the Pre-Upgrade Report
4	Ensure that `getPlatformTransactionManager()` method is not used in custom code.	See, Ensuring That getPlatformTransactionManager() Method is Not Used in Custom Code
5	Empty the `oimProcessQueue` JMS queue to ensure that JMS messages are processed before you start upgrading.	See, Emptying the oimProcessQueue JMS Queue
6	Complete all of the pre-requisite tasks.	See, Other Prerequisites
7	Ensure that the JRF is upgraded.	See, Ensuring That JRF is Upgraded
8	In Oracle Identity Manager 11.1.1.x.x, if you do not have at least one reconciliation field of type `IT Resource`, then you must create one for all account type profiles.	See, Creating Reconciliation Field of Type IT Resource
9	Back up your environment.	See, Backing Up Oracle Identity Manager 11g Release 1 (11.1.1.x.x)

Table 11–1 (Cont.) Upgrade Flow

Sl No	Task	For More Information
10	Set the JVM properties for the Oracle Identity Manager Server(s) using the WebLogic Administration console.	See, Setting JVM Properties for Oracle Identity Manager Server(s)
11	Shut down all servers. This includes Administration Server, SOA Managed Servers, and Oracle Identity Manager Managed Servers.	See, Shutting Down Node Manager, Administration Server and Managed Servers
	Upgrading the Oracle Home and Database Schemas	
12	Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6.	See, Upgrading Oracle WebLogic Server
13	Upgrade SOA suite used by Oracle Identity Manager.	See, Upgrading Oracle SOA Suite to 11.1.1.7.0
14	Upgrade Oracle Identity Manager binaries to 11.1.2.2.0.	See, Upgrading Oracle Identity Manager Binaries to 11.1.2.2.0
15	Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load OPSS schema for Oracle Identity and Access Management products.	See, Creating Oracle Platform Security Services Schema
16	Upgrade the Oracle Platform Security Services schemas.	See, Upgrading Oracle Platform Security Services Schemas
17	Extend your Oracle Identity Manager 11.1.1.x.x domain with the OPSS template.	See, Extending Oracle Identity Manager 11.1.1.x.x Component Domains with OPSS Template
18	Upgrade Oracle Platform Security Services.	See, Upgrading Oracle Platform Security Services
19	Run the `configuresecuritystore.py` script to configure policy stores.	See, Configuring OPSS Security Store
20	Upgrade Oracle Identity Manager using the Patch Set Assistant.	See, Upgrading Oracle Identity Management Schemas Using Patch Set Assistant
21	Start the WebLogic Administration Server and the SOA Managed Server(s).	See, Starting the Administration Server and SOA Managed Server
	Upgrading the Oracle Identity Manager Middle Tier	
22	Upgrade Oracle Identity Manager Middle Tier.	See, Upgrading Oracle Identity Manager Middle Tier
23	Verify the Oracle Identity Manager Middle Tier Upgrade.	See, Verifying Oracle Identity Manager Middle Tier Upgrade
24	Change the deployment order of Oracle Identity Manager from 47 to 48.	See, Changing the Deployment Order of Oracle Identity Manager EAR
25	Restart the Administration Server and SOA Managed Servers.	See, Restarting the Administration Server and SOA Managed Server

Table 11–1 (Cont.) Upgrade Flow

Sl No	Task	For More Information
26	Patch the Oracle Identity Manager MDS metadata by starting the Oracle Identity Manager Managed Servers.	See, Patching Oracle Identity Management MDS Metadata
	Upgrading Other Oracle Identity Manager Installed Components	
27	Upgrade Oracle Identity Manager Design Console.	See, Upgrading Oracle Identity Manager Design Console
28	Upgrade Oracle Identity Manager Remote Manager.	See, Upgrading Oracle Identity Manager Remote Manager
29	Configure Oracle BI Publisher 11g Release 1 (11.1.1.7.1).	See, Configuring Oracle BI Publisher 11.1.1.7.1
30	Deploy the Oracle Identity Manager BI Publisher Reports.	See, Deploying Oracle Identity Manager BI Publisher Reports
	Post-Upgrade Steps	
31	Complete the post-upgrade steps.	See, Post-Upgrade Steps
32	Verify the upgrade.	See, Verifying the Upgrade

11.2 Pre-Upgrade

This section contains the following topics:

- Feature Comparison
- Reviewing System Requirements and Certification
- Generating and Analyzing the Pre-Upgrade Report
- Ensuring That getPlatformTransactionManager() Method is Not Used in Custom Code
- Emptying the oimProcessQueue JMS Queue
- Other Prerequisites
- Ensuring That JRF is Upgraded
- Creating Reconciliation Field of Type IT Resource
- Backing Up Oracle Identity Manager 11g Release 1 (11.1.1.x.x)
- Setting JVM Properties for Oracle Identity Manager Server(s)
- Shutting Down Node Manager, Administration Server and Managed Servers

11.2.1 Feature Comparison

Table 11–2 lists the key differences in functionality between Oracle Identity Manager 11.1.1.x.x and 11*g* Release 2 (11.1.2.2.0).

Table 11–2 Features Comparison

Oracle Identity Manager 11.1.1.5.0 and/or 11.1.1.7.0	Oracle Identity Manager 11.1.2.2.0
Oracle Identity Manager 11.1.1.x.x provided Identity Attestation to periodically review a user's access. For advanced access review capabilities such as role or data owner certification, OIM 11.1.1.x had to be integrated with Oracle Identity Analytics (OIA) to leverage the advanced access review capabilities that OIA provided.	In Oracle Identity Manager 11.1.2.1.0 and 11.1.2.2.0, the advanced access review capabilities of OIA are converged into OIM to provide a complete identity governance platform that enables an enterprise to do enterprise grade access request, provisioning, and access review from a single product. After upgrading to Oracle Identity Manager 11.1.2.2.0, you can use the new access review capabilities. This feature is disabled by default. Therefore, you must ensure that you have relevant licenses before enabling this new feature.
In Oracle Identity Manager 11.1.1.x.x, users are assigned to organizations by specifying an organization name in the `Organization` attribute of the user details. This is a static organization membership. A user can only be a member of one organization.	In Oracle Identity Manager 11.1.2.2.0, in addition to the existing feature, you can dynamically assign users to organizations based on user-membership rules, which you can define in the **Members** tab of the organization details page. All users who satisfy the user-membership rule are dynamically associated with the organization, irrespective of the organization hierarchy the users statically belong to. With this new capability, a user can gain membership of one home organization via static membership and multiple secondary organizations via user-membership rules that are dynamically evaluated.
In Oracle Identity Manager 11.1.1.x.x, administrators configured request templates to control what an end user could request. End users have to navigate through a series of menus to select entitlement before they can submit and access request. An end user's access to request templates was controlled by his/her role memberships.	Oracle Identity Manager 11.1.2.2.0 provides a new user interface with a shopping cart-type request model through which end users can search and browse through the catalog and directly request any item such as roles, entitlements, or applications, without having to navigate through a series of menus. In addition to this, several business-friendly metadata such as description, audit objective, tags, owner, approver, technical glossary, and so on can be associated to each access item, to display business-friendly and rich contextual information to a business user at the time of self service access request and access review. An end user's access to entities is controlled by a combination of user-to-organization publishing and entity-to-organization publishing. Post upgrade, administrators need to run the catalog synchronization job to populate the catalog with request-*able* entities and entity metadata. Post upgrade, administrators need to define entity to organization publishing to control what an end user can request.

Table 11–2 (Cont.) Features Comparison

Oracle Identity Manager 11.1.1.5.0 and/or 11.1.1.7.0	Oracle Identity Manager 11.1.2.2.0
Resource and IT resource names tend to be named in a manner that makes it easy for the IT users to manage them. The problem with this approach is that if a business user has to request access, the resource name will not make sense. These incomprehensible Resource and IT resource names make the access request process non-intuitive.	Oracle Identity Manager 11.1.2.2.0 provides an abstraction entity called Application Instance. It is a combination of IT resource instance (target connectivity and connector configuration) and resource object (provisioning mechanism). Administrators can assign business-friendly names to Application instances and map them to corresponding IT resources and Resource Objects. End users who request for accounts through the catalog will search for an account by providing the business-friendly Application Instance Name. Application instances are automatically created as part of the upgrade procedure. Administrators are expected to define organization publishing for these Application Instances to control who has access to requests for access to the application.
In Oracle Identity Manager 11.1.1.x.x, authorization policies are used to control a user's access to the functions within Oracle Identity Manager. Policy administration was done through a UI that was built specifically for Oracle Identity Manager.	Oracle Identity Manager 11.1.2.2.0 leverages Oracle Entitlement Server for authorization policy enforcement and administration. This is the standards-based platform for authorization policy enforcement and administration across all IDM components. Administration of Authorization Policies is now done through the Authorization Policy Manager, which is the main tool for lifecycle management of Authorization Policies. Post upgrade to Oracle Identity Manager 11.1.2.2.0 authorization policy definition and administration will have to be done from the Authorization Policy Manager console and any customizations made to out of the box 11.1.1.x authorization policies will have to be reapplied.
In Oracle Identity Manager 11.1.1.x.x, access to policy evaluation is done instantly for each user when they are updated.	In Oracle Identity Manager 11.1.2.2.0, access to policy evaluation is done when the Evaluate User Policies scheduled job is run. This gives you the flexibility to control when heavy operations such as access policy evaluation and provisioning are triggered. Post upgrade to Oracle Identity Manager 11.1.2.2.0, administrators will have to schedule this job to run in predefined intervals based on their business requirements.

Table 11–2 (Cont.) Features Comparison

Oracle Identity Manager 11.1.1.5.0 and/or 11.1.1.7.0	Oracle Identity Manager 11.1.2.2.0
Oracle Identity Manager 11.1.1.x.x provided separate interfaces for end user self-service and delegated administration.	In Oracle Identity Manager 11.1.2.2.0, the end user self-service and delegated administration consoles have been unified into a single self service console to simplify administration and self service. Oracle Identity Manager 11.1.2.2.0 also uses the Skyros skin, which is a light weight skin. Any customization added to the 11.1.1.x.x User Interface (UI) will have to be reapplied on the 11.1.2.2.0 User Interface post upgrade. For an overview of UI customization in Oracle Identity Manager 11.1.2.2.0, see "Customizing the Interface" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

11.2.2 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements for the products you are installing or upgrading. For more information see Section 2.1, "Reviewing System Requirements and Certification".

11.2.3 Generating and Analyzing the Pre-Upgrade Report

You must run the pre-upgrade utility before you begin the upgrade process, and address all the issues listed as part of this report with the solution provided in the report.

The pre-upgrade utility analyzes your existing Oracle Identity Manager 11.1.1.x.x environment, and provides information about the mandatory prerequisites that you must complete before you upgrade environment. The information in the pre-upgrade report is related to the invalid approval policies, requests and event handlers that are affected by the upgrade, list of mandatory Database components that need to be installed before upgrade, cyclic groups in LDAP directory, deprecated authorization policies, and issues in creating potential application instance.

> **Note:** It is important to address all the issues listed in the pre-upgrade report, before you can proceed with the upgrade, as upgrade might fail if the issues are not fixed.
>
> Run this report until no pending issues are listed in the report.

To generate and analyze the pre-upgrade report, complete the tasks described in the following sections:

- Obtaining Pre-Upgrade Report Utility
- Generating the Pre-Upgrade Report
- Analyzing Pre-Upgrade Report

11.2.3.1 Obtaining Pre-Upgrade Report Utility

You must download the pre-upgrade utility from Oracle Technology Network (OTN). The utility is available in two zip files named `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002`, along with `ReadMe.doc` at the following location on My Oracle Support:

My Oracle Support document ID 1599043.1.

The `ReadMe.doc` contains information about how to generate and analyze the pre-upgrade reports.

11.2.3.2 Generating the Pre-Upgrade Report

To generate the pre-upgrade report for Oracle Identity Manager 11.1.1.x.x upgrade, do the following:

1. Create a directory at any location and extract the contents of `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002` in the newly created directory.
2. Create a directory where pre-upgrade reports need to be generated. For example, name the directory *`OIM_preupgrade_reports`*.
3. Go to the directory where you extracted `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002`, and open the `preupgrade_report_input.properties` file in a text editor. Update the properties file by specifying the appropriate values for the parameters listed in Table 11–3:

Table 11–3 Parameters to be Specified in the preupgrade_report_input.properties File

Parameter	Description
`oim.targetVersion`	Specify `11.1.2.2.0` for this parameter, as `11.1.2.2.0` is the target version for which pre-upgrade utility needs to be run.
`oim.jdbcurl`	Specify the JDBC URL for Oracle Identity Manager in the following format: *`<host>:<port>/<service_name>`*
`oim.oimschemaowner`	Specify the name of the OIM schema owner.
`oim.mdsjdbcurl`	Specify the MDS JDBC URL in the following format: *`<host>:<port>/<service_name>`*
`oim.mdsschemaowner`	Specify the name of the MDS schema owner.
`oim.databaseadminname`	Specify the user with DBA privilege. For example, `sys as sysdba`.
`oim.outputreportfolder`	Specify the absolute path to the directory that you created in step-2 (directory with name *`OIM_preupgrade_reports`*), where the pre-upgrade reports need to be generated. Make sure that the output report folder has read and write permissions.
`oim.oimhome`	Specify the absolute path to the OIM Home.
`oim.wlshome`	Specify the absolute path to the WLS Home.

*Table 11–3 (Cont.) Parameters to be Specified in the preupgrade_report_*

Parameter	Description
oim.domain	Specify the absolute path to the Oracle Identity Manager domain home. For example: /Middleware/user_projects/domains/base_domain

4. Set the environment variables JAVA_HOME, MW_HOME, WL_HOME, and OIM_HOME by running the following commands:

   On UNIX:

   ```
   export JAVA_HOME=<jdk_location>
   export MW_HOME=<absolute_path_to_middleware_home>
   export OIM_HOME=<absolute_path_to_middleware_home>/Oracle_IDM1/
   export WL_HOME=<absolute_path_to_middleware_home>/WL_HOME/
   ```

   On Windows:

   ```
   set JAVA_HOME="<jdk_location>"
   set MW_HOME="<absolute_path_to_middleware_home>"
   set OIM_HOME="<absolute_path_to_middleware_home>\Oracle_IDM1\"
   set WL_HOME="<absolute_path_to_middleware_home>\WL_HOME\"
   ```

5. Run the following command from the location where you extracted the contents of PreUpgradeReport.zip.001 and PreUpgradeReport.zip.002:

   - **On UNIX**:

     ```
     sh generatePreUpgradeReport.sh
     ```

   - **On Windows**:

     ```
     generatePreUpgradeReport.bat
     ```

6. Provide the details when the following is prompted:

   - **OIM Schema Password**

     You must enter the password of the OIM schema.

   - **MDS Schema Password**

     You must enter the password of the MDS schema.

   - **DBA Password**

     You must enter the password of the Database Administrator.

The following are the reports generated by the pre-upgrade report utility:

Pre-Upgrade Reports Generated for 11.1.1.x.x Starting Point

- index.html
- APPROVALPOLICYPreUpgradeReport.html
- ChallengeQuesPreUpgradeReport.html
- CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html
- DomainReassocAuthorization.html

- EVENT_HANDLERPreUpgradeReport.html
- ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html
- ORACLE_ONLINE_PURGE_PreUpgradeReport.html
- PasswordPolicyPreUpgradeReport.html
- PROVISIONINGBYREQUESTPreUpgradeReport.html
- PROVISIONINGPreUpgradeReport.html
- REQUESTPreUpgradeReport.html
- UDFPreUpgradeReport.html
- WLSMBEANPreUpgradeReport.html

11.2.3.3 Analyzing Pre-Upgrade Report

The PreUpgradeReport utility generates several reports, which are outlined in Table 11–4.

Note: You must review all the reports, and perform the tasks described in each of the reports.

Table 11–4 Pre-Upgrade Utility Reports

Report Name	Description	For More Information
index.html	The index.html provides links to all the seven reports generated by the pre-upgrade utility.	-
APPROVALPOLICYPreUpgradeReport.html	This report lists the request approval policies that has a rule defined on the non existing template.	See, Description of APPROVALPOLICYPreUpgradeReport.html Report
ChallengeQuesPreUpgradeReport.html	This report provides information about upgrading localized challenge questions data. When you upgrade Oracle Identity Manager 11.1.1.x.x to 11.1.2.2.0, the existing localization data for challenge questions is lost. Therefore, before proceeding with the upgrade process, you must backup the existing localized challenge questions data. After you upgrade to Oracle Identity Manager 11.1.2.2.0, you must perform the tasks described in this report.	See, Description of ChallengeQuesPreUpgradeReport.html Report

Table 11–4 (Cont.) Pre-Upgrade Utility Reports

Report Name	Description	For More Information
CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html	This report detects the list of cyclic groups in LDAP. The report includes a list of cyclic groups and instructions to remove cyclic dependency. It is mandatory to remove all cyclic dependencies running in the Oracle Identity Manager 11.1.1.x.x environment.	See, Description of CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html Report
DomainReassocAuthorization.html	This report lists the checks executed for authorization feature data upgrade. It checks if the Oracle Identity Manager is reassociated with the DB-based policy store. Review the table that lists the checks executed and the status of the checks.	See, Description of DomainReassocAuthorization.html Report
EVENT_HANDLERPreUpgradeReport.html	This report captures all user customizations related to Event Handler in Oracle Identity Manager 11.1.1.x.x.	See, Description of EVENT_HANDLERPreUpgradeReport.html Report
ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html	This report provides the status of the mandatory database components or settings for Oracle Identity Manager upgrade. Verify the installation or setup status for each of the mandatory component or setting. If any of the component or setting is not setup correctly, follow the recommendations provided in the report to fix them. **Note**: This report will not be generated if there is no action item related to purge.	See, Description of ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html Report
ORACLE_ONLINE_PURGE_PreUpgradeReport.html	This report lists the pre-requisites for Online Purge that needs to be addressed before you proceed with the upgrade. **Note**: This report will not be generated if there is no action item related to purge.	See, Description of ORACLE_ONLINE_PURGE_PreUpgradeReport.html Report
PasswordPolicyPreUpgradeReport.html	This report lists the potential upgrade issues for password policies.	See, Description of PasswordPolicyPreUpgradeReport.html Report
PROVISIONINGBYREQUESTPreUpgradeReport.html	This report lists the requests that are not viewable in Track Requests page.	See, Description of PROVISIONINGBYREQUESTPreUpgradeReport.html Report
PROVISIONINGPreUpgradeReport.html	This report lists the potential application instance creation issues.	See, Description of PROVISIONINGPreUpgradeReport.html Report

Table 11–4 (Cont.) Pre-Upgrade Utility Reports

Report Name	Description	For More Information
REQUESTPreUpgradeReport.html	This report lists any invalid requests and the actions to be taken.	See, Description of REQUESTPreUpgradeReport.html Report
UDFPreUpgradeReport.html	This report provides information about the steps that must be performed prior to upgrade to ensure that the User Defined Fields (UDFs) are upgraded seamlessly.	See, Description of UDFPreUpgradeReport.html Report
WLSMBEANPreUpgradeReport.html	This report provides information about the status of mandatory deletion of OIM Authenticator Jar(s).	See, Description of WLSMBEANPreUpgradeReport.html Report

11.2.3.3.1 Description of APPROVALPOLICYPreUpgradeReport.html Report

The report `APPROVALPOLICYPreUpgradeReport.html` lists the invalid approval policies. This report contains the following sections:

- Approval Policy rule defined on template
- List of Approval Polices which needs to be updated with custom approval process
- Approval policy based on unsupported request type

This report also contains an additional note on approval policy based on deprecated request type. You must review the report completely, before you start upgrading the Oracle Identity Manager 11.1.1.x.x environment.

Approval Policy rule defined on template

This section lists the Oracle Identity Manager 11.1.1.x.x approval policies whose rules are defined based on the request template.

The Request templates feature is not supported in Oracle Identity Manager 11.1.2.2.0. Therefore, if your Oracle Identity Manager 11.1.1.x.x contains approval policies having rules based on request template, you must reconfigure the request approval policies by following the steps described in the report.

List of Approval Polices which needs to be updated with custom approval process

This section lists the 11.1.1.x.x approval policies that need to be associated with different approval process before you start the upgrade process.

The approval process `default/ResourceAdministratorApproval`, `default/ResourceAuthorizerApproval` are not supported in 11.1.2.2.0. Therefore, if your Oracle Identity Manager 11.1.1.x.x contains approval policies having these approval process, you must associate them with different approval process.

Approval policy based on unsupported request type

This section provides information about the request types that are not supported in 11.1.2.2.0.

The following 11.1.1.x.x request types are not supported in 11.1.2.2.0, and they are changed to non-self request type in 11.1.2.2.0:

- Self Assign Roles

- Modify Self Profile
- Self Remove Roles
- Self De-Provision Resource
- Self Modify Provisioned Resource
- Self-Request Resource

Self-request type mapping to Non-Self request type is shown Table 11–5.

Table 11–5 Mapping of Self request type to Non-Self request type

Self Request Type	Non-Self Request Type
Self-Request Resource	Provision Resource
Self Modify Provisioned Resource	Modify Provisioned Resource
Self Remove Roles	Remove from Roles
Modify Self Profile	Modify User Profile
Self De-Provision Resource	De-Provision Resource
Self Assign Roles	Assign Roles

Approval policy based on deprecated request type

This section provides information about deprecated request types in 11.1.2.2.0.

The following 11.1.1.x.x request types are deprecated in 11.1.2.2.0:

- Provision Resource
- De-Provision Resource
- Disable Provisioned Resource
- Enable Provisioned Resource
- Modify Provisioned Resource

Approval policies based on these deprecated request types will continue to work for any pending requests based on these request types even after upgrade. But, these policies will not work for requests created for Application Instance based request types such as - Provision ApplicationInstance, Revoke Account, Disable Account, Enable Account, and Modify Account.

In addition, approval policies for Application Instance based request types need to be explicitly created for the request based on Application Instance.

11.2.3.3.2 Description of ChallengeQuesPreUpgradeReport.html Report

The report `ChallengeQuesPreUpgradeReport.html` is generated for both 11.1.2 and 11.1.2.1.0 starting points.

When you upgrade Oracle Identity Manager 11.1.2.x.x to 11.1.2.2.0, the existing localization data for challenge questions is lost as it is not upgrade-safe. Therefore, before you upgrade to Oracle Identity Manager 11.1.2.2.0, you must backup the existing localized challenge questions data.

After you upgrade to 11.1.2.2.0, perform the tasks described in this report to localize challenge questions. Follow the instructions in the section applicable for your starting point.

Note: If you have already migrated the localized challenge questions data per localization model provided in Oracle Identity Manager 11*g* Release 2 (11.1.2.0.11) or (11.1.2.1.3), ignore the tasks described in this report.

11.2.3.3.3 Description of CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html Report

The report `CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html` provides information about the Cyclic groups in LDAP directory.

Oracle Identity Manager 11.1.2.2.0 does not support cyclic groups in the LDAP directory. Therefore, you must remove the cyclic dependency from Oracle Identity Manager 11.1.1.x.x setup and reconcile data from LDAP to Oracle Identity Manager Database, before you proceed with the upgrade. For more information about removing the cyclic groups dependent on LDAP, see Removing Cyclical Groups Dependent on LDAP and Reconciling Data From LDAP to OIM Database. The procedure for removing cyclic groups is also described in this report.

Removing Cyclical Groups Dependent on LDAP and Reconciling Data From LDAP to OIM Database

If the LDAP in your Oracle Identity Manager 11.1.1.x.x environment has cyclic groups loaded, you must remove the cyclic groups by doing the following:.

1. Use JEXplorer or Softerra LDAP Administrator and navigate to the cyclic groups.
2. Look for **uniquemember** attribute.
3. Remove all values from the attribute.
4. Save the group.
5. Reconcile the data from LDAP to Oracle Identity Manager Database by running the following command:

   On UNIX: `LDAPConfigPostSetup.sh`

   On Windows: `LDAPConfigPostSetup.bat`

Example Scenario

If you have cyclic group dependency between two groups: Group1 and Group2, do the following to remove cyclic dependency:

1. Connect to LDAP using JEXplorer or Softerra LDAP.
2. Go to the group container of Group1.
3. Go to the **uniquemember** attribute under Group1.
4. Remove the value of Group2, from unique members, and save the change made.
5. Run `LDAPConfigPostSetup.sh` on UNIX and `LDAPConfigPostSetup.bat` on Windows to synchronize data from LDAP to Oracle Identity Manager database.

11.2.3.3.4 Description of DomainReassocAuthorization.html Report

The report `DomainReassocAuthorization.html` is generated for both 11.1.2 and 11.1.2.1.0 starting points.

It checks if the Oracle Identity Manager domain is reassociated to Database based policy store and displays the result in the **Result** column. Review the checks executed and the result of the checks.

11.2.3.3.5 Description of EVENT_HANDLERPreUpgradeReport.html Report The report `EVENT_HANDLERPreUpgradeReport.html` provides information about event handlers. When you upgrade Oracle Identity Manager 11.1.1.x.x to Oracle Identity Manager 11.1.2.2.0, the customizations made to the OOTB event handlers XMLs in 11.1.1.x.x will not be preserved in 11.1.2.2.0. All the customizations defined in a separate XML (non OOTB) in 11.1.1.x.x will be preserved in 11.1.2.2.0. You must redo all the customizations after upgrading to 11.1.2.2.0. This report contains the following sections:

- New Event Handler Added by the customer in the OOTB (11.1.1.5.0) Event Handler Metadata XML
- OOTB(11.1.1.5.0) Event Handler modified by the Customer
- OOTB(11.1.1.5.0) Event Handler deleted by Customer

Refer to the table in the report for more details about the event handlers.

New Event Handler Added by the customer in the OOTB (11.1.1.5.0) Event Handler Metadata XML

This section provides information about the new event handlers added in the OOTB (11.1.1.5.0).

The event handler newly added in the OOTB (11.1.1.5.0) Event Handler Metadata XML will not be available after you upgrade to 11.1.2.2.0. Oracle Identity Manager 11.1.2.2.0 event handlers will replace the 11.1.1.x.x event handlers. Therefore, you must add the event handler again in a new file after the upgrade.

> **Note:** Do not add new event handler in the same OOTB Event Handler XML. You must create a new XML and add the new event handler to it.

OOTB(11.1.1.5.0) Event Handler modified by the Customer

This section provides information about the event handlers that are modified in the OOTB (11.1.1.5.0).

You must redo all the customizations that you did to the event handlers in OOTB (11.1.1.5.0), after you upgrade Oracle Identity Manager 11.1.1.x.x to 11.1.2.2.0.

OOTB(11.1.1.5.0) Event Handler deleted by Customer

This section provides information about the event handlers that were deleted in OOTB (11.1.1.5.0).

The deleted event handlers are restored after you upgrade to 11.1.2.2.0. Therefore, you must delete them again as per requirement.

11.2.3.3.6 Description of ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html Report The report `ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html` is generated for both 11.1.2 and 11.1.2.1.0 starting points.

This report lists all the mandatory database components or settings for Oracle Identity Manager 11.1.2.x.x upgrade. This report contains a table which lists the component or setting, it's installation or setup status, and recommendations if any. You must review the installation or setup status for each of the mandatory component or setting listed in the table. If the component or setting is not setup correctly, follow the recommendations specified in the **Note** column of the table in the report to fix them.

11.2.3.3.7 Description of ORACLE_ONLINE_PURGE_PreUpgradeReport.html Report Before you upgrade Oracle Identity Manager 11.1.2.x.x to 11.1.2.2.0, you must complete the pre-requisites for online purge.

The table in this report lists the database tables on which the mentioned pre-upgrade steps need to be performed before you upgrade. The table also shows the status of the database tables in **OIM schema** and **Note** section. Review the table, and perform the actions required.

11.2.3.3.8 Description of PasswordPolicyPreUpgradeReport.html Report If you are using 9.1.x.x password policy model you must update to new password policies. The 9.1.x.x password policy model is no longer supported for `Users`, and any such customizations done are not migrated to the new password policy model.

Following password policies are attached to the `Xellerate User` resource object according to the 9.1.x.x password policy model and must be assigned to appropriate organization(s):

Table 11–6 Password Policies

Policy Key	Policy Name
1	Default Policy

11.2.3.3.9 Description of PROVISIONINGBYREQUESTPreUpgradeReport.html Report The following table provides information about the requests that are not viewable in Track Requests page:

Table 11–7 Password Policies

Request Key	Beneficiary Key	Entity Type	Entity Name	Entity Key	Request Model Name	Issue
81	83	Resource	AD User	7	Access Policy Based Provisioning	No process form entry found for process instance. Cannot update `rbe_entity_key` in `request_beneficiary_entities` table since application instance for the entry is not created.
82	85	Resource	AD User	7	Access Policy Based Provisioning	No process form entry found for process instance. Cannot update `rbe_entity_key` in `request_beneficiary_entities` table since application instance for the entry is not created.
86	99	Resource	AD User	7	Provision Resource	No process form entry found for process instance. Cannot update `rbe_entity_key` in `request_beneficiary_entities` table since application instance for the entry is not created.

11.2.3.3.10 Description of PROVISIONINGPreUpgradeReport.html Report The report PROVISIONINGPreUpgradeReport.html lists the potential application instances creation issues. The report contains the following sections:

- Provisioning, Entitlement, and Access Policy Configuration Details
- List of Resource Objects without Process Form
- List of Resource Objects without ITResource field Type in Process Form
- List of Resource Objects with multiple ITResource Lookup fields in Process Form
- List of Access Policies without ITResource value set in default policy data

- List of Access Policies with Revoke If No Longer Applies flag unchecked
- List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value

Provisioning, Entitlement, and Access Policy Configuration Details

This sections describes the steps you must complete before you upgrade Oracle Identity Manager 11.1.1.x.x to 11.1.2.2.0. These steps are related to provisioning, entitlement, and access policy configuration. Complete all the steps described in this section of the report.

List of Resource Objects without Process Form

This section provides information about the resource objects in Oracle Identity Manager 11.1.1.x.x that do not have process form. Each resource object must have a process form associated with it. Therefore, if a resource object is not associated with a process form, you must associate the resource object with a process form before you start the upgrade process. Review the table in this section of the report, that lists the details of the resource objects without process form.

List of Resource Objects without ITResource field Type in Process Form

This section provides information about the resource objects without ITResource field type in their respective process forms. Review the table in this section of the report, which contains more details. If your Oracle Identity Manager 11.1.1.x.x has resource objects without ITResource field in their process forms, do the following:

1. Create appropriate IT resource definition.
2. Create IT resource instance for the same corresponding to the target that is being provisioned.
3. Edit the process form and add a field of type "`ITResource`" to the process form. Set the following properties:

   `Type=`*`IT Resource definition created in step-1`*

   `ITResource=true`
4. Activate the form.
5. Update the IT resource field on existing provisioned accounts using FVC Utility.
6. Once the above steps are completed, you can create application instances corresponding to the Resource Object+ITResource combination.

List of Resource Objects with multiple ITResource Lookup fields in Process Form

This section provides information about the resource objects that have multiple lookup fields in their process form. In the Oracle Identity Manager 11.1.1.x.x environment, if you have resource objects with multiple ITResource set in the process form, you must set the value of the property `ITResource Type` to `true` for at least one of the attributes.

List of Access Policies without ITResource value set in default policy data

This section lists the access policies for which the ITResource values of the resource objects should be set in the default policy data. The table in this section lists the access policies in Oracle Identity Manager 11.1.1.x.x for which ITResource field is missing. You must set the values of ITResource field for each of the access policy listed in the table.

List of Access Policies with Revoke If No Longer Applies flag unchecked

This section lists the access policies that have `Revoke If No Longer Applies` flag unchecked. The table in this section contains the list of access policies that will be updated to `Disable If No Longer Applies`, during upgrade. The table also indicates if tasks for `enable`, `disable`, `revoke` actions are not defined for these policies. You must add the missing tasks before you proceed with the upgrade. Also, if you want the behavior of the policy to change to RNLA checked, you must check the RNLA flag for the respective policy.

List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value

This section lists entitlements stored in lookup definitions that do not have IT Resource Key pretended to their encoding values using "~". Entitlements stored in lookup definitions need IT Resource Key prepended to the encoded values using "~". Review the table in this section of the pre-upgrade report, which contains more details.

11.2.3.3.11 Description of REQUESTPreUpgradeReport.html Report The report `REQUESTPreUpgradeReport.html` lists requests that are affected because of the upgrade. This report contains the following sections:

- Requests with unsupported request stages
- Requests which will be automatically changed to corresponding non-self request type

Requests with unsupported request stages

This section lists the requests that are in one of the following unsupported request stages:

- Obtaining Template Approval
- Template Approval Approved
- Template Approval Rejected
- Template Approval Auto Approved

Manual intervention is required to move these requests to the next stage by approving, withdrawing, or closing such requests. Otherwise, requests are moved to `request closed` stage as part of the upgrade.

Review the list of requests that are in the unsupported request stage.

Requests which will be automatically changed to corresponding non-self request type

This section lists the requests that are based on one of the following request types will be changed to the corresponding non-self request type after the upgrade:

- Self Assign Roles
- Modify Self Profile
- Self Remove Roles
- Self De-Provision Resource
- Self Modify Provisioned Resource
- Self-Request Resource

Request types for these requests are automatically changed to the corresponding non-self request type as part of the upgrade.

Self-request type mapping to non-self request type is shown in Table 11–8:

Table 11–8 Mapping of Self-Request Type to Non-Self Request Type

Self request type	Non-Self request type
Self-Request Resource	Provision Resource
Self Modify Provisioned Resource	Modify Provisioned Resource
Self Remove Roles	Remove from Roles
Modify Self Profile	Modify User Profile
Self De-Provision Resource	De-Provision Resource
Self Assign Roles	Assign Roles

11.2.3.3.12 Description of UDFPreUpgradeReport.html Report This section provides information about the steps that must be performed prior to upgrade to ensure that the User Defined Fields/Attributes (UDFs) are upgraded seamlessly. Note that you may have to edit the entity xml file manually. To edit a file in MDS, you need to export the file from Metadata Services (MDS) repository and after making the required changes file must be imported back to MDS.

The following table lists the path of the entity xml file in MDS corresponding to a particular entity type.

Table 11–9 Path of Entity XML File in MDS

Entity type	Path in MDS
User	/file/User.xml
Role	/db/identity/entity-definition/Role.xml
Organization	/db/identity/entity-definition/Organization.xml

The report also includes information about the list of UDFs with inconsistent max-size and UDFs with inconsistent default value.

11.2.3.3.13 Description of WLSMBEANPreUpgradeReport.html Report The Jar(s) present in WebLogic Server mbeans path must be deleted before executing Mid-Tier Upgrade as listed in the below table.

Table 11–10 Jars and their Status

File Name	Status
`OIMAuthenticator.jar`	`OIMAuthenticator.jar` is present.
`oimsignaturembean.jar`	`oimsignaturembean.jar` is present.
`oimsigmbean.jar`	`oimsigmbean.jar` is not present.

Note: As a pre-upgrade step, delete the Jars `OIMAuthenticator.jar` and `oimsignaturembean.jar` from `<MW_HOME>/wlserver_10.3/server/lib/mbeantypes/.`

11.2.4 Ensuring That getPlatformTransactionManager() Method is Not Used in Custom Code

Ensure that the method `getPlatformTransactionManager()` is not used in the custom event handler code, as this method is not available in 11.1.2.2.0.

If you are using the method getPlatformTransactionManager() in the custom event handler code, set the attribute `tx` to `TRUE` in the event handler XML definition.

For more information on setting the attributes in the event handler XML definition, see "Defining Custom Events Definition XML" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

11.2.5 Emptying the oimProcessQueue JMS Queue

Offline Provisioning is not supported in Oracle Identity Manager 11.1.2.2.0, as it is no longer needed on Oracle Identity Manager 11.1.2.2.0.

Empty the `oimProcessQueue` JMS queue to ensure that JMS messages are processed before you start upgrading. To do so, complete the following:

1. Shut down applications to disable accessing of Oracle Identity Manager offline provisioning by end-users, SPML, and API clients.
2. Monitor the `oimProcessQueue` JMS queue from the Weblogic Administration Console and allow Oracle Identity Manager to run, till `oimProcessQueue` JMS queue is empty.

11.2.6 Other Prerequisites

This is a list of checks you must run and set before you begin upgrading:

- Check if `oracle.soa.worklist.webapp` is targeted to Oracle Identity Manager server in 11.1.1.x.x. If not, target it to Oracle Identity Manager Managed Server. If you are upgrading Oracle Identity Manager high availability environments, you must target `oracle.soa.worklist.webapp` to the `oim_cluster`.
- The OOTB applications in Oracle Identity Manager are deployed in `NO_STAGE` mode. Check if `oracle.idm.uishell` is in `No Stage` mode. If `oracle.idm.uishell` is in `Stage` mode, you must re-deploy it to `NO_STAGE` mode.

  Complete the following steps to change the mode to `No Stage`:

  1. Set the *`WL_HOME`* and *`OIM_HOME`*.
  2. Undeploy `oracle.idm.uishell` by running the following command:

     ```
     java -cp $WL_HOME/server/lib/weblogic.jar weblogic.Deployer
     -adminurl t3://localhost:8005 -username weblogic -password
     weblogic1 -undeploy -name oracle.idm.uishell
     ```

  3. Deploy `oracle.idm.uishell` in stage mode by running the following command:

     ```
     java -cp $WL_HOME/server/lib/weblogic.jar weblogic.Deployer
     -adminurl t3://localhost:8005 -username weblogic -password
     weblogic1 -deploy -name oracle.idm.uishell -source $OIM_
     HOME/modules/oracle.idm.uishell_11.1.1/oracle.idm.uishell.war
     -nostage -library -targets AdminServer,$OIM_SERVER_NAME
     ```

- Ensure that all pending requests are addressed before you upgrade.

- In case of a migrated, upgraded, or restored database in the Oracle Identity Manager environment, you must synchronize all the Oracle Identity Manager Schema Privileges (SYSTEM and OBJECT Grants) from the source to the target (restored) schema by doing the following:

  1. Capture the OIM Database Schema user constituent grants from the source schema by executing the following SQLs as `SYS` database user:

     – `SELECT DBMS_METADATA.GET_GRANTED_DDL ('SYSTEM_GRANT','<OIM_Schema_Name>') FROM DUAL;`

     – `SELECT DBMS_METADATA.GET_GRANTED_DDL ('OBJECT_GRANT', '<OIM_Schema_Name>') FROM DUAL;`

  2. In the schema restoration phase prior to schema upgrade, execute the grants output of the SQLs captured in step-1, as post schema restoration step.

  3. Recompile any `INVALID` objects in the OIM schema using the following steps:

     a. Identify `INVALID` schema objects as `SYS` user by running the following SQL:

     ```
     SELECT owner,object_type,object_name,status FROM dba_objects WHERE
     status = 'INVALID' AND owner in ('<OIM_Schema_Name1>') ORDER BY
     owner, object_type, object_name;
     ```

     b. Compile the `INVALID` schema objects using any appropriate method. The following is an example of compiling `INVALID` schema objects by executing the method `UTL_RECOMP` as `SYS` user for the OIM schema:

     ```
     UTL_RECOMP.recomp_serial('<OIM_Schema_Name>');

     END;
     ```

     Repeat step-a until there are no `INVALID` objects.

Note: For information on schema backup and restoration using Data Pump Client Utility for Oracle Identity Manager 11*g* Release 1, see My Oracle Support document ID 1359656.1.

For information on schema backup and restoration using Data Pump Client Utility for Oracle Identity Manager 11*g* Release 2, see My Oracle Support document ID 1492129.1.

11.2.7 Ensuring That JRF is Upgraded

Before starting the upgrade process, you must ensure that Java Required Files (JRF) is upgraded. To do this, complete the following steps:

1. Log in to the WebLogic Administration console using the following URL:

   `http://host:port/console`

   In this URL, *host* refers to the name of the host on which WebLogic Administration Server is running, and *port* refers to the port number.

2. Click **Deployments** on the left navigation pane for the *OIM_Domain*.

3. Ensure that the following libraries are present:

   - `oracle.adf.desktopintegration(1.0,11.1.1.2.0)`
   - `oracle.adf.desktopintegration.model(1.0,11.1.1.2.0)`
   - `oracle.bi.adf.model.slib(1.0,11.1.1.2.0)`

- `oracle.bi.adf.view.slib(1.0,11.1.1.2.0)`
- `oracle.bi.adf.webcenter.slib(1.0,11.1.1.2.0)`
- `oracle.bi.composer(11.1.1,0.1)`
- `oracle.bi.jbips(11.1.1,0.1)`

If the above libraries are not present, you must upgrade JRF. For more information about upgrading JRF, see "Updating Fusion Middleware Shared Libraries" in the *Oracle Fusion Middleware Patching Guide*.

11.2.8 Creating Reconciliation Field of Type IT Resource

All account reconciliation Field Mapping configurations must have at least one Reconciliation field of type `ITResource` defined. This can be done by adding a mapping from the Oracle Identity Manager Design Console. Complete the following steps for those resource objects which do not have `ITResource` filed in reconciliation field mapping:

1. Create reconciliation field of type `IT Resource` by doing the following:
   a. Log in to the Oracle Identity Manager Design Console by running the following command from the location *`ORACLE_HOME`*`/designconsole/`:

      On UNIX: `./xlclient.sh`

      On Windows: `xlclient.cmd`

   b. Expand **Resource Management**.
   c. Click **Resource Objects**.
   d. Search for and select the Resource Object that you wish to modify.
   e. Go to the **Object Reconciliation** tab.
   f. Click **Add Field** under **Reconciliation Fields** tab.
   g. Enter the Field Name, and select **IT Resource** as the **Field Type**.
   h. Click Save icon.
2. Define mapping for the field `ITResource` by doing the following:
   a. On the Oracle Identity Manager Design Console, expand **Process Management** on the left navigation pane.
   b. Click **Process Definition**.
   c. Go to the **Reconciliation Field Mapping** tab in the **Process Definition** form.
   d. Search for the Resource Object.
   e. Define mapping for the field **IT Resource**.
   f. Save the form.

Note: This step is required if you are using connector for account reconciliation or if you wish to use connector for account reconciliation after you upgrade to 11.1.2.2.0.

11.2.9 Backing Up Oracle Identity Manager 11g Release 1 (11.1.1.x.x)

You must back up your old Oracle Identity Manager 11.1.1.x.x environment before you upgrade to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0).

After stopping the servers, back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Identity Manager schemas
- MDS schema
- ORASDPM schema
- SOAINFRA schemas

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

11.2.10 Setting JVM Properties for Oracle Identity Manager Server(s)

You must set additional JVM properties for the Oracle Identity Manager Server(s) using the WebLogic Administration console. To do this, complete the following steps:

1. Log in to the WebLogic Administration console using the following URL:

   `http://admin_host:admin_port/console`

2. Click **Servers**.
3. Select the Oracle Identity Manager server.
4. Click **Server Start**, and then click **Arguments**.
5. Add the following application module settings for the Oracle Identity Manager Server(s):

   ```
   -Djbo.ampool.doampooling=true

   -Djbo.ampool.minavailablesize=1

   -Djbo.ampool.maxavailablesize=120

   -Djbo.recyclethreshold=60

   -Djbo.ampool.timetolive=-1

   -Djbo.load.components.lazily=true

   -Djbo.doconnectionpooling=true

   -Djbo.txn.disconnect_level=1

   -Djbo.connectfailover=false

   -Djbo.max.cursors=5

   -Doracle.jdbc.implicitStatementCacheSize=5

   -Doracle.jdbc.maxCachedBufferSize=19
   ```

Note: The recommended values for the arguments specified assume 100 concurrent users per node. Therefore, the value specified for the argument `-Djbo.ampool.maxavailablesize` is `120` (that is, `100 * 1.20`). If the number of concurrent users per node is different, use the following formula to calculate the value that you must specify for the argument `-Djbo.ampool.maxavailablesize`:

```
-Djbo.ampool.maxavailablesize = <Number_of_concurrent_users>
* 1.20
```

6. Restart the Oracle Identity Manager Server(s). To restart Managed Server(s), stop the server(s) first and start them again.

   For more information about stopping a Managed Server, see Section 2.8.1, "Stopping the Managed Server(s)".

   For more information about starting a Managed Server, see Section 2.9.3, "Starting the Managed Server(s)".

11.2.11 Shutting Down Node Manager, Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Managed Servers, Administration Server, and the Node Manager.

Note: When shutting down the servers, the following error message might be displayed:

```
** SOA specific environment is already set. Skipping ...
**********************************************************
OIM specific environment is already set. Skipping ...
The input line is too long.
The syntax of the command is incorrect.
```

It is recommended that you open a new command prompt and then run the commands for shutting down the servers.

For information about stopping the servers, see "Stopping the Servers" on page 2-10.

11.3 Upgrade Procedure

This section describes different tasks involved in the upgrade process, like upgrading Oracle Identity Manager and Oracle SOA Suite 11.1.1.x.x binaries, creating 11.1.2.2.0 schemas, configuring the security store, upgrading the Oracle Identity Manager middle tier, verifying the upgrade and so on. The tasks in this section should be performed after you complete all the prerequisites described in section Pre-Upgrade.

This section contains the following topics:

- Upgrading Oracle WebLogic Server
- Upgrading Oracle SOA Suite to 11.1.1.7.0
- Upgrading Oracle Identity Manager Binaries to 11.1.2.2.0
- Creating Oracle Platform Security Services Schema

- Upgrading Oracle Platform Security Services Schemas
- Extending Oracle Identity Manager 11.1.1.x.x Component Domains with OPSS Template
- Upgrading Oracle Platform Security Services
- Configuring OPSS Security Store
- Upgrading Oracle Identity Management Schemas Using Patch Set Assistant
- Starting the Administration Server and SOA Managed Server
- Upgrading Oracle Identity Manager Middle Tier
- Verifying Oracle Identity Manager Middle Tier Upgrade
- Changing the Deployment Order of Oracle Identity Manager EAR
- Restarting the Administration Server and SOA Managed Server
- Patching Oracle Identity Management MDS Metadata
- Upgrading Oracle Identity Manager Design Console
- Upgrading Oracle Identity Manager Remote Manager
- Configuring Oracle BI Publisher 11.1.1.7.1
- Deploying Oracle Identity Manager BI Publisher Reports

11.3.1 Upgrading Oracle WebLogic Server

You can upgrade WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6 by using the WebLogic 10.3.6 Upgrade Installer. For information about upgrading Oracle WebLogic Server, see "Upgrading to Oracle WebLogic Server 10.3.6" on page 2-2.

11.3.2 Upgrading Oracle SOA Suite to 11.1.1.7.0

Note: Oracle Identity Manager 11.1.2.2.0 supports Oracle SOA Suite 11.1.1.7.0. Therefore, you must upgrade Oracle SOA Suite to 11.1.1.7.0 if you are not using Oracle SOA Suite 11.1.1.7.0 already.

Oracle Identity Manager 11.1.1.5.0 uses Oracle SOA Suite 11.1.1.5.0, and Oracle Identity Manager 11.1.2.2.0 uses Oracle SOA Suite 11.1.1.7.0. Therefore, this task is needed only if you are upgrading Oracle Identity Manager 11.1.1.5.0 to 11.1.2.2.0.

For information about applying the mandatory Oracle SOA Suite patches for Oracle Identity Manager 11.1.1.7.0, see "Mandatory Patches Required for Installing Oracle Identity Manager" in the *Oracle Fusion Middleware Release Notes*.

To upgrade your existing Oracle SOA Suite to 11.1.1.7.0, complete the tasks listed in Table 11–11:

Table 11–11 Tasks to Update SOA

Sl No	Task	For More Information
1	Review the system requirements and specifications before you start upgrading Oracle SOA Suite to 11.1.1.7.0.	See, Oracle Fusion Middleware System Requirements and Specifications
2	Obtain the Oracle SOA Suite 11.1.1.7.0 installer.	See, *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*
3	Start the Oracle SOA Suite 11.1.1.7.0 installer.	See, "Start the Installer" in the *Oracle Fusion Middleware Patching Guide*
4	Update the Oracle SOA Suite binaries to 11.1.1.7.0.	See, "Applying the Patch Set" in the *Oracle Fusion Middleware Patching Guide*
5	Apply the mandatory Oracle SOA Suite patches.	See, "Mandatory Patches Required for Installing Oracle Identity Manager" in the *Oracle Fusion Middleware Release Notes*
6	Perform the following post-patching tasks for Oracle SOA Suite: ■ Remove the `tmp` folder for SOA composer, BPM workspace, and B2B. ■ If you upgraded Oracle SOA Suite 11*g* Release 1 (11.1.1.6.0) to 11*g* Release 1 (11.1.1.7.0), update the message duration of the warning `BPEL Message Recovery Required`. ■ Update the `MAXRECOVERATTEMPT` attribute to `2`. ■ Update your Oracle Data Integrator clients if you are using Oracle BAM and Oracle Data Integrator integration. ■ Save and restore XEngine customizations for Oracle B2B, if B2B server is integrated with B2B EDI endpoints. ■ Extending the SOA domain with UMS Adapter features. ■ Extend the SOA domain with Business Process Management features Make sure you have started the WebLogic Administration Server and the SOA Managed Servers before you perform the post-patching tasks.	See the following sections in the *Oracle Fusion Middleware Patching Guide* for 11*g* Release 1 (11.1.1.7.0): ■ Removing the tmp Folder for SOA Composer, BPM Workspace and B2B ■ Updating the "BPEL Message Recovery Required" Warning Message Duration ■ Updating MAXRECOVERATTEMPT Attribute to 2 ■ Updating the Oracle Data Integrator Clients if BAM-ODI Integration is Enabled ■ Saving and Restoring XEngine Customizations for Oracle B2B ■ Extending the SOA Domain with UMS Adapter Features ■ Extending the SOA Domain with Business Process Management Features Post-patching tasks for SOA are not required out-of-the-box. However, you must review them and apply per your functional requirements.

11.3.3 Upgrading Oracle Identity Manager Binaries to 11.1.2.2.0

To upgrade Oracle Identity Manager binaries to 11.1.2.2.0, you must use the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Installer. During the procedure, point the Middleware Home to your existing 11.1.1.x.x Middleware Home. Your Oracle Home is upgraded from 11.1.1.x.x to 11.1.2.2.0.

Note: Before upgrading the Oracle Identity Manager binaries to 11*g* Release 2 (11.1.2.2.0), you must ensure that the OPatch version in *ORACLE_HOME* and *MW_HOME*/oracle_common is 11.1.0.9.9. Different OPatch version might cause patch application failure. If you have upgraded opatch to a newer version, you will have to roll back to version 11.1.0.9.9.

For information about upgrading Oracle Identity Manager 11g Release 1 (11.1.1.x.x), see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

After the binary upgrade, check the installer logs at the following location:

- On UNIX: *ORACLE_INVENTORY_LOCATION*/logs

  To find the location of the Oracle Inventory directory on UNIX, check the file *ORACLE_HOME*/oraInst.loc.

- On Windows: *ORACLE_INVENTORY_LOCATION*\logs

  The default location of the Oracle Inventory Directory on Windows is C:\Program Files\Oracle\Inventory\logs.

The following install log files are written to the log directory:

- install*DATE-TIME_STAMP*.log
- install*DATE-TIME_STAMP*.out
- installActions*DATE-TIME_STAMP*.log
- installProfile*DATE-TIME_STAMP*.log
- oraInstall*DATE-TIME_STAMP*.err
- oraInstall*DATE-TIME_STAMP*.log

11.3.4 Creating Oracle Platform Security Services Schema

You must create Oracle Platform Security Services (OPSS) schema using Repository Creation Utility (RCU) 11.1.2.2.0, as Oracle Identity Manager upgrade process involves OPSS schema policy store changes. Keys, roles, permissions, and other artifacts used by the applications must migrate to the policy store.

To create OPSS schema using Repository Creation utility, do the following:

1. Obtain the RCU.

   For information about obtaining the RCU software, see *Oracle Identity and Access Management Download, Installation, and Configuration ReadMe* for 11*g* Release 2 (11.1.2.2.0).

2. Start the RCU.

   For information about starting the RCU, see "Starting RCU" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

3. Create the OPSS schema.

   For information about creating schemas, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

Note: In the **Select Components** screen, expand **AS Common Schemas** and select **Oracle Platform Security Services**. Make sure you do not select any other components.

The **Metadata Services** schema is selected automatically. Deselect it and ignore the following message:

```
Following components require Metadata Services schema:
Oracle Platform Security Services.
```

11.3.5 Upgrading Oracle Platform Security Services Schemas

You must upgrade the Oracle Platform Security Services schemas using Patch Set Assistant. To do this, complete the following steps:

Note: Before you upgrade Oracle Platform Security Services schemas, make sure that you have execute privileges to the `SOAINFRA` schema owner on `sys.dbms_lob`. If not, grant execute privileges to the `SOAINFRA` schema owner on `sys.dbms_lob` by running the following command:

```
grant execute on sys.dbms_lob to *_SOAINFRA;
```

1. Start the Patch Set Assistant from the location *`MW_HOME`*`/oracle_common/bin` using the following command:

   ```
   ./psa
   ```

2. Select **opss**.

3. Specify the Database connection details, and select the schema to be upgraded.

After you upgrade Oracle Platform Security Services schema, verify the upgrade by checking the log file at the location *`MW_HOME`*`/oracle_common/upgrade/logs/psa<`*`timestamp`*`>.log`.

The *`timestamp`* refers to the actual date and time when Patch Set Assistant was run. If the upgrade fails, check the log files to rectify the errors and run the Patch Set Assistant again.

11.3.6 Extending Oracle Identity Manager 11.1.1.x.x Component Domains with OPSS Template

Oracle Identity Manager 11.1.2.2.0 uses the database to store Oracle Platform Security Service policies. This requires extending the 11.1.1.x.x Oracle Identity Manager domain to include the OPSS data source.

To do so, complete the following steps:

1. Run the following command to launch the Oracle Fusion Middleware configuration wizard:

   On UNIX:

   ```
   ./config.sh
   ```

   It is located in the `<MW_HOME>/<Oracle_IDM1>/common/bin` directory.

   On Windows:

`config.cmd`

It is located in the `<MW_HOME>\<Oracle_IDM1>\common\bin` directory.

2. On the **Welcome** screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
3. On the **Select a WebLogic Domain Directory** screen, browse to the directory that contains the WebLogic domain in which you configured the components. Click **Next**. The **Select Extension Source** screen is displayed.
4. On the **Select Extension Source** screen, select the **Oracle Platform Security Service - 11.1.1.0 [Oracle_IDM1]** option. After selecting the domain configuration options, click **Next**.
5. The **Configure JDBC Data Sources** screen is displayed. Configure the opssDS data source, as required. After the test succeeds, the **Configure JDBC Component Schema** screen is displayed.
6. On the **Configure JDBC Component Schema** screen, select the **Oracle Platform Security Services** schema.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**.

   The **Test JDBC Component Schema** screen is displayed. After the test succeeds, the **Select Optional Configuration** screen is displayed.
7. On the **Select Optional Configuration** screen, you can configure Managed Servers, Clusters, and Machines and Deployments and Services. Do not select anything as you have already configured in your Oracle Identity Manager 11.1.1.x.x environment. Click **Next**.
8. On the **Configuration Summary** screen, review the domain configuration, and click **Extend** to start extending the domain.

Your existing Oracle Identity Manager domain is extended to support Oracle Platform Security Services (OPSS).

11.3.7 Upgrading Oracle Platform Security Services

After you extend the Oracle Identity Manager component domains with OPSS template, you must upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Identity Manager to 11.1.2.2.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see Section 2.7, "Upgrading Oracle Platform Security Services".

11.3.8 Configuring OPSS Security Store

You must configure the database Security Store as it is the only security store type supported by Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0). This is done by running the `configureSecurityStore.py` script.

For information about configuring Oracle Platform Security Services, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

11.3.9 Upgrading Oracle Identity Management Schemas Using Patch Set Assistant

You must upgrade Oracle Identity Manager schema using Patch Set Assistant (PSA). When you select the Oracle Identity Manager Schema, it automatically selects all dependent schemas and upgrades them too.

For information about upgrading schemas using the Patch Set Assistant, see Upgrading Schemas Using Patch Set Assistant.

After you upgrade schemas, verify the upgrade by checking the version numbers of the schemas as described in Version Numbers After Upgrading Schemas.

11.3.9.1 Version Numbers After Upgrading Schemas

Run `select version,status,upgraded from schema_version_registry where owner=<SCHEMA_NAME>;` and ensure that the version numbers are upgraded, as listed in Table 11–12:

Table 11–12 Component Version Numbers After Upgrading the Schemas

Component	Version No.
OPSS	11.1.1.7.2
MDS	11.1.1.7.0
Oracle Identity Manager	11.1.2.2.0
ORASDPM	11.1.1.7.0
SOAINFRA	11.1.1.7.0 (Make sure that you have upgraded SOA schemas as described in Section 2.6, "Upgrading Schemas Using Patch Set Assistant")

11.3.10 Starting the Administration Server and SOA Managed Server

Note: Do not start the Oracle Identity Manager Managed Servers.

After the upgrade is complete, start the WebLogic Administration Server, the Administration Server for the domain that contains Oracle Identity Management, and SOA Managed Server.

Note: If you are upgrading Oracle Identity Manager high availability environments and if you are using Oracle Automatic Storage Management Cluster File System (Oracle ACFS), you must start only one SOA Managed Server before running the middle tier upgrade utility.

Note: When you start the servers, the following error message might be displayed:

```
** SOA specific environment is already set. Skipping ...
**********************************************************
OIM specific environment is already set. Skipping ...
The input line is too long.
The syntax of the command is incorrect.
```

It is recommended that you open a new command prompt and then run the commands for starting the servers.

For information about starting the Administration Server and SOA Managed server, see Section 2.9, "Starting the Servers".

11.3.11 Upgrading Oracle Identity Manager Middle Tier

To upgrade the Oracle Identity Manager middle tier, you must update the properties file with the necessary parameters, and then run the command as described in this section.

Note: Before you upgrade the Oracle Identity Manager middle tier, make sure that the WebLogic Administration Server and the SOA Managed Server(s) are running. It is recommended that the Oracle Identity Manager Managed Server is not running at this point.

Note: The execution is re-entrant and will resume with correct execution even if there is any interruption in between.

To upgrade Oracle Identity Manager Middle Tier to 11.1.2.2.0, do the following:

On UNIX:

1. Move from your present working directory to the `<OIM_ORACLE_HOME>/server/bin` directory by running the following command on the command line:

   ```
   cd <OIM_ORACLE_HOME>/server/bin
   ```

2. Edit the following upgrade properties file in a text editor:

   ```
   oim_upgrade_input.properties
   ```

3. Add the parameters, as listed in Table 11–13.

4. Run the following command:

   ```
   ./OIMUpgrade.sh
   ```

   When you run this command, you will need to enter password for OIM schema user, MDS schema user, WebLogic admin user and SOA admin user.

Note: The following warning is displayed:

```
[WARN] [jrockit] PermSize=128M ignored: Not a valid option
for JRockit

[WARN] [jrockit] MaxPermSize=256M ignored: Not a valid
option for JRockit
```

You can ignore this message.

On Windows:

1. Move from your present working directory to the `<OIM_ORACLE_HOME>\server\bin` directory by running the following command on the command line:

   ```
   cd <OIM_ORACLE_HOME>\server\bin
   ```

2. Edit the following upgrade properties file in a text editor:

   ```
   oim_upgrade_input.properties
   ```

3. Add the parameters, as listed in Table 11–13.

4. Run the following command:

   ```
   OIMUpgrade.bat
   ```

   When you run this command, you will need to enter password for OIM schema user, MDS schema user, WebLogic admin user and SOA admin user.

Note: The following warning is displayed:

```
[WARN] [jrockit] PermSize=128M ignored: Not a valid option
for JRockit

[WARN] [jrockit] MaxPermSize=256M ignored: Not a valid
option for JRockit
```

You can ignore this message.

Table 11–13 Oracle Identity Manager Middle Tier Upgrade Parameters

Parameter	Description
`java.home`	Specify the JAVA HOME location.
`server.type`	Specify the Application Server that you are using. For example, if you are using Oracle WebLogic Server, specify `wls` for this parameter. As this document describes the procedure to upgrade Oracle Identity Manager on WebLogic, you must specify `wls` for this parameter.
`oim.jdbcurl`	Specify the Oracle Identity Manager JDBC URL.
`oim.oimschemaowner`	Specify the Oracle Identity Manager schema owner.
`oim.oimmdsjdbcurl`	Specify the MDS JDBC URL.
`oim.mdsschemaowner`	Specify the MDS schema owner name.
`oim.adminhostname`	Specify the Oracle WebLogic Server Administration host name.
`oim.adminport`	Specify the Oracle WebLogic Server Administration port.

Table 11–13 (Cont.) Oracle Identity Manager Middle Tier Upgrade Parameters

Parameter	Description
oim.adminUserName	Specify the username that is used to log in to the Oracle WebLogic Server Administration Console.
oim.soahostmachine	Specify the SOA host name where SOA Server is running.
oim.soaportnumber	Specify the SOA Server port.
oim.soausername	Specify the SOA Managed Server username.
oim.domain	Specify the Oracle Identity Manager domain location.
oim.home	Specify the Oracle OIM Home location.
oim.mw.home	Specify the Oracle Middleware Home location.
soa.home	Specify the Oracle SOA Home location.
wl.home	Specify the WebLogic Home location.

Example Parameters

```
java.home=/u01/jrockit-jdk1.6.0_24-R28.1.3-4.0.1
server.type=wls
oim.jdbcurl=db.example.com:1522:oimdb
oim.oimschemaowner=test_oim
oim.oimmdsjdbcurl=db.example.com:1522:oimdb
oim.mdsschemaowner=test_mds
oim.adminport=7001
oim.adminhostname=oimhost.example.com
oim.adminUserName=weblogic
oim.soahostmachine=soahost.example.com
oim.soaportnumber=8001
oim.soausername=weblogic
oim.domain=/scratch/Oracle/Middleware/user_projects/domains/base_domain
oim.home=/scratch/Oracle/Middleware/Oracle_IDM1
oim.mw.home=/scratch/Oracle/Middleware
soa.home=/scratch/Oracle/Middleware/Oracle_SOA1
wl.home=/scratch/Oracle/Middleware/wlserver_10.3
```

11.3.12 Verifying Oracle Identity Manager Middle Tier Upgrade

Complete the following steps to verify the Oracle Identity Manager Middle Tier upgrade:

1. Verify the log files at the following location, by looking for error or warning messages:

   On UNIX:

   `<OIM_HOME>/server/upgrade/logs/MT`

   On Windows:

   `<OIM_HOME>\server\upgrade\logs\MT`

   The following log files are generated:

   - `ant_ApplicationDB.log`
   - `ant_grantPermissionsUpgrade.log`
   - `ant_JRF.log`

- ant_PatchClasspath.log
- ant_soaOIMLookupDB.log
- OIMUpgrade<timestamp>.log
- SeedSchedulerData.log

No error message is displayed if the middle tier upgrade was successful.

2. OIMupgrade.sh creates a detailed report. Complete the following steps to verify the Oracle Identity Manager Middle Tier upgrade:

   a. Go to the following path:

      On UNIX:

      <Oracle_IDM1>/server/upgrade/logs/MT/oimUpgradeReportDir

      On Windows:

      <Oracle_IDM1>\server\upgrade\logs\MT\oimUpgradeReportDir

   b. Click **index.html**.

      This contains list of all Oracle Identity Manager features and upgrade status of the last middle tier run, in a table format.

   c. Click on the corresponding link of each feature for a detailed feature report.

Table 11–14 Middle Tier Upgrade Report

Feature	Name	Description
	index.html	This report provides a list of features and their upgrade status, from the last run. Access the detailed feature report through the corresponding link on each feature.
PatchDomain	PatchDomain.html	This report provides details of all domain related changes during the upgrade process. The changes are: ■ New EAR or shared libraries deployed during the upgrade process. ■ New server resources. ■ Foreign JNDI Provider Creation. ■ Application of upgrade template for creating the following resources: – New data sources For example: Application DBDS – jrf-async queuesDomain Classpath Upgrade ■ OPSS upgrade. ■ JRF upgrade.
ROLE_RULE_MEMB	PS1R2UPG.ROLE_RULE_MEMB.html	This report provides details of roles processed on the basis of Search Rule, prepared from Rule Elements, defined in the Rules.

Table 11–14 (Cont.) Middle Tier Upgrade Report

Feature	Name	Description
REQUEST_ STAGES	PS1R2UPG.REQUEST_ STAGES.html	The following request stages are no longer supported: ■ Obtaining Template Approval ■ Template Approval Approved ■ Template Approval Rejected ■ Template Approval Auto Approved This report lists the following: ■ Requests for unsupported request stages, processed during upgrade. ■ Tasks associated to request with unsupported request stages, processed during upgrade. ■ SOA tasks associated to request with unsupported request stages, processed during upgrade.
ReconUpgrade	ReconUpgradeUpgrade Report.html	This report lists object names processed during upgrade with names of the associated Horizontal Table Name, Recon Profile Name, and Entity Definition Name.
SOAUpgrade	NA	New OOTB SOA Composites deployed: ■ sca_DisconnectedProvisioning_rev1.0.jar ■ sca_DefaultSODApproval_rev1.0.jar
Scheduler	NA	This report lists the addition of the following Task Definition's and Scheduler Jobs: ■ Account Application Instance Update Task. ■ Catalog Synchronization Task. ■ Application Instance Post Delete. Processing Task. ■ Entitlement Post Delete Processing Task.
ACCESSPOLICY	ACCESSPOLICYUpgrade Report.html	This report provides a list of access policy names and the corresponding resource objects, processed during upgrade along with DNLA flag value. Set the value as 1 if DNLA is set, 0 if RNLA is set.
MDSNSUpdate	NA	Oracle Identity Manager Metadata present in Oracle Identity Manager MDS is updated with the latest namespace to keep them in consoance with changes in XSD Schemas.
OIMConfig	NA	Oracle Identity Manager Application configuration, kept in the metadata location /db/oim-config.xml, is updated as per the latest configuration changes in Oracle Identity Manager 11.1.2.2.0.
CONTEXT	NA	DDL changes in the ORCHPRCESS TABLE. Data from the old context columns (ContextId) is transformed and moved to new context column (ContextVal).
Certificatio n	CertificationUpgrad eReport.html	This report provides a list of the certification records processed during the upgrade of snapshot data.
Request	PS12R2UPG.InflightR equest.html	This report provides the list of the requests that are in request or operational level approval stage. In addition, the report provides upgrade status.

Table 11–14 (Cont.) Middle Tier Upgrade Report

Feature	Name	Description
InflightRequest	REFIX_NOT_AVLBL.InflightRequest.html	This report provides the list of the inflight requests in 11.1.1.x.x requests that are in either request or operational level approval stage. In addition, the report provides upgrade status.
PREFIX_NOT_AVLBL_ReconUpgrade	PREFIX_NOT_AVLBL.ReconUpgrade.html	This report provides the list of the success/failure of 11.1.2.2.0-based Recon Profile creation for the resource objects defined in 11.1.1.x.x.
PREFIX_NOT_AVLBL_ACCESSPOLICY	PREFIX_NOT_AVLBL.ACCESSPOLICY.html	This report provides the list of the access policy names and the corresponding resource objects processed during upgrade along with DNLA flag value (set to 1 if DNLA is set, 0 if RNLA is set).

11.3.13 Changing the Deployment Order of Oracle Identity Manager EAR

You must change the deployment order of `oim.ear` from 47 to 48. Complete the following steps to do so:

1. Log in to the WebLogic console.
2. Click **Deployments** in the left pane.
3. Click **oim.ear**.
4. Update the deployment order from 47 to 48, click **Save**.

11.3.14 Restarting the Administration Server and SOA Managed Server

To restart the Administration Server and Managed Servers, you must stop them first before starting them again.

To stop the servers, see Shutting Down Node Manager, Administration Server and Managed Servers.

To start the servers, see Starting the Administration Server and SOA Managed Server.

Things to Check on the WebLogic Console After Starting the Administration Server

- Check the new data source added:
  1. Log in to Weblogic console.
  2. Click **Data Sources**.
  3. Verify the data source data source given below:

Name	Type	JNDI Name	Targets
ApplicationDBDS	Generic	jdbc/ApplicationDBDS	oim_server1 (for single node upgrade) oim_cluster (for cluster upgrade)

- Check for SOA Foreign JNDI provider
  1. Log in to Weblogic console.
  2. Click **Foreign JNDI Providers**.

3. Verify the existence of Foreign JNDI providers given below:

Name	Initial Context Factory	Provider URL	User	Targets

ForeignJNDIProvider-SOA	weblogic.jndi.WLInitialContextFactory	For single node upgrade:
		`t3://soa_server_host:soa_server_port`
		For cluster upgrade:
		`t3://soa_server1_host:soa_server1_port,soa_server2_host:soa_server2_port`
			WebLogic	`oim_server1` (for single node upgrade)
				`oim_cluster` (for cluster upgrade)

Note: If you are upgrading Oracle Identity Manager High Availability environments, the Provider URL may contain the host and port of `soa_server1` only. In that case, you must add the host and port of `soa_server2` to the Provider URL manually.

- Check the order of the EARs
  1. Log in to Weblogic console.
  2. Click **Deployments**.
  3. Verify the deployment order for the following list respectively:

Name	State	Health	Type	Deployment Order
oim (11.1.1.3.0)	Active	OK	Enterprise Application	48
OIMAppMetadata (11.1.2.0.0)	Active	OK	Enterprise Application	47
OIMMetadata (11.1.1.3.0)	Active	OK	Enterprise Application	46
oracle.iam.console.identity.sysadmin.ear (V2.0)	Active	OK	Enterprise Application	406
oracle.iam.console.identity.self-service.ear (V2.0)	Active	OK	Enterprise Application	405
oracle.iam.ui.custom(11.1.1,11.1.1)	Active		Library	404
oracle.iam.ui.oia-view(11.1.1,11.1.1)	Active		Library	403

Name	State	Health	Type	Deployment Order
oracle.iam.ui.view(11.1.1,11.1.1)	Active		Library	402
oracle.iam.ui.model(1.0,11.1.1.5.0)	Active		Library	401

11.3.15 Patching Oracle Identity Management MDS Metadata

Oracle Identity Manager 11.1.1.x.x MDS metadata must be upgraded to Oracle Identity Manager 11.1.2.2.0 MDS metadata. Starting the Oracle Identity Manager Managed Servers patches the MDS metadata.

To start the Managed Servers, do the following:

On UNIX:

1. Move from your present working directory to the `<MW_HOME>/user_projects/domains/<domain_name>/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/user_projects/domains/<domain_name>/bin
   ```

2. Run the following command to start the Servers:

   Note: Enter the username and password when prompted.

   ```
   ./startManagedWebLogic.sh <managed_server_name>
   ```

   where

   `<managed_server_name>` is the name of the Managed Server.

On Windows:

1. Move from your present working directory to the `<MW_HOME>\user_projects\domains\<domain_name>\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\user_projects\domains\<domain_name>\bin
   ```

2. Run the following command to start the Managed Servers:

   Note: Enter the username and password when prompted.

   ```
   startManagedWebLogic.cmd <managed_server_name>
   ```

   where

   `<managed_server_name>` is the name of the Managed Server.

For more information, see "Starting the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Verifying MDS Patch

Check MDS reports in the following location:

On UNIX:

```
<OIM_ORACLE_HOME>/server/logs/MDS_REPORT_DIRECTORY/MDSReport.html
```

On Windows:

```
<OIM_ORACLE_HOME>\server\logs\MDS_REPORT_DIRECTORY\MDSReport.html
```

11.3.16 Upgrading Oracle Identity Manager Design Console

The Oracle Identity Manager Design Console is used to configure system settings that control the system-wide behavior of Oracle Identity Manager and affect its users. The Design Console allows you to perform user management, resource management, process management, and other administration and development tasks.

Oracle recommends that you install Oracle Identity Manager and the Design Console in different directory paths, if the Design Console is on the same system as Oracle Identity Manager server.

To upgrade Design Console, complete the following steps:

1. Back up the following files:
   - On UNIX, `$<XLDC_HOME>/xlclient.sh`
   - `$<XLDC_HOME>/config/xlconfig.xml`
   - On Windows, `<XLDC_HOME>\xlclient.cmd`
   - `<XLDC_HOME>\config\xlconfig.xml`
2. Run the Oracle Identity and Access Management 11.1.2.2.0 Installer to upgrade the Design Console home `<XLDC_HOME>`.

   For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
3. Restore the backed up files `xlclient.sh/xlclient.cmd` and `xlconfig.xml` to the upgrade design console home.
4. Build and copy the `wlfullclient.jar` file as follows:
   a. Go to `WebLogic_Home/server/lib` directory on UNIX and `WebLogic_Home\server\lib` directory on Windows.
   b. Set the `JAVA_HOME` environment variable and add the `JAVA_HOME` variable to the `PATH` environment variable.

      For example, you can set the `JAVA_HOME` to the `jdk160_21` directory inside the Middleware home.

      On UNIX:

      ```
      setenv JAVA_HOME $MW_HOME/jdk160_29
      ```

      On Windows:

      ```
      SET JAVA_HOME=<MW_HOME>\jdk160_29
      ```
   c. Run the following command to build the `wlfullclient.jar` file:

      ```
      java -jar <MW_HOME>/modules/com.bea.core.jarbuilder_1.7.0.0.jar
      ```
   d. Copy the `wlfullclient.jar` file to the `<IAM_HOME>` where you installed the Design Console. For example:

      On UNIX:

      ```
      cp wlfullclient.jar <Oracle_IDM2>/designconsole/ext
      ```

      On Windows:

```
copy wlfullclient.jar <Oracle_IDM2>\designconsole\ext
```

11.3.17 Upgrading Oracle Identity Manager Remote Manager

Complete the following steps to upgrade Remote Manager:

1. Back up configuration files.

   Before starting the Remote Manager upgrade, back up the following Remote Manager configuration files:

   - On UNIX, `$<XLREMOTE_HOME>/remotemanager.sh`
   - `$<XLREMOTE_HOME>/xlremote/config/xlconfig.xml` file.
   - On Windows, `<XLREMOTE_HOME>\remotemanager.bat`
   - `<XLREMOTE_HOME>\xlremote\config\xlconfig.xml` file.

2. Run the Oracle Identity and Access Management Installer to upgrade the Remote Manager home.

   For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2.2.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

3. Restore the backed up configuration files, `remotemanager.sh`/`remotemanager.bat` and `xlconfig.xml`, in the upgraded Remote Manager home.

11.3.18 Configuring Oracle BI Publisher 11.1.1.7.1

To use reports on Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0), you must install Oracle BI Publisher 11*g* Release 1 (11.1.1.7.1). To install Oracle BI Publisher 11*g* Release 1 (11.1.1.7.1), you must first install Oracle BI Publisher 11*g* Release 1 (11.1.1.7.0), and then apply the patch for Oracle BI Publisher 11*g* Release 1 (11.1.1.7.1) using OPATCH. To do this, complete the following steps:

1. Back up the following Oracle Identity Manager reports directories:

   - *$BI_PUBLISHER_HOME*`/Middleware/user_projects/domains/bifoundation_domain/config/bipublisher/repository/Reports/Oracle Identity Manager/`
   - *$ORACLE_BI_PUBLISHER_HOME*`/Middleware/user_projects/domains/bifoundation_domain/config/bipublisher/repository/Reports/BIP Sample Data/`

   Note: The location of Oracle Business Intelligence Reports directory may differ based on the installation location of BI Publisher.

2. Obtain Oracle BI Publisher 11*g* Release 1 (11.1.1.7.0) from the following location:

   http://www.oracle.com/technetwork/middleware/bi-enterprise-edition/downloads/bi-downloads-1923016.html

3. Install Oracle BI Publisher 11*g* Release 1 (11.1.1.7.0). For more information about installing Oracle BI Publisher 11*g* Release 1 (11.1.1.7.0), see *Oracle Fusion Middleware Installation Guide for Oracle Business Intelligence*.

4. Apply the patch number `16556157` to patch Oracle BI Publisher 11*g* Release 1 (11.1.1.7.0) to Oracle BI Publisher 11*g* Release 1 (11.1.1.7.1). The patch `16556157` can be downloaded at the following URL:

https://support.oracle.com

For patching instructions, refer to the README.txt file that is provided with the patch.

Note: For more information about deploying BI Reports, see "Deploying Oracle Identity Manager Reports" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

For more information about using the reporting features, see "Using Reporting Features" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

11.3.19 Deploying Oracle Identity Manager BI Publisher Reports

Complete the following steps to deplpoy Oracle Identity Manager BI Publisher Reports:

1. Obtain the reports bundle oim_product_BIP11gReports_11_1_2_0_0.zip. from the following location:

   MW_HOME/I*AM_HOME*/server/reports/oim_product_BIP11gReports_11_1_2_0_0.zip

2. Unzip oim_product_BIP11gReports_11_1_2_0_0.zip at the following location:

   IAM_HOME/Middleware/user_projects/domains/*domain_name*/config/bipublisher/repository/Reports/

3. Configure reports by following the instructions in "Configuring Oracle Identity Manager Reports" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

11.4 Post-Upgrade Steps

This section contains the following topics:

- After You Upgrade
- Validating the Database Objects
- Creating sysadmin Key
- Impact of Removing Approver-Only Attribute in Request Data Set
- Changes to Request API After Upgrading to Oracle Identity Manager 11g Release 2 (11.1.2.2.0)
- Enabling Oracle Identity Manager-Oracle Access Manager Integration After Upgrading to Oracle Identity Manager 11g Release 2 (11.1.2.2.0)
- Running the Entitlement List Schedule
- Running the Evaluate User Policies Scheduled Task
- Running Catalog Synchronization
- UMS Notification Provider
- Upgrading User UDF
- Upgrading Application Instances
- Redeploying XIMDD

- Redeploying SPML-DSML
- Customizing Event Handlers
- Upgrading SOA Composites
- Provisioning Oracle Identity Management Login Modules Under WebLogic Server Library Directory
- Reviewing Performance Tuning Recommendations
- Authorization Policy Changes
- Creating Password Policies
- Creating PeopleSoft Enterprise HRMS Reconciliation Profile
- Reviewing OIM Data Purge Job Parameters
- Migrating Customized Oracle Identity Manager Reports
- Reviewing Connector Certification
- Verifying the Functionality of Connectors
- Updating the Provider URL For ForeignJNDIProvider-SOA
- Verifying the Upgrade

11.4.1 After You Upgrade

After upgrading from Oracle Identity Manager 11.1.1.x.x to Oracle Identity Manager 11.1.2.2.0:

- The name of the following EARs remain unchanged from Oracle Identity Manager 11.1.1.x.x to Oracle Identity Manager 11.1.2.2.0:
  - Oracle Identity Manager Metadata (11.1.1.3.0)
  - Oracle Identity Manager (11.1.1.3.0)

  There is no functional loss.
- All of the resources provisioned to an organization in Oracle Identity Manager 11.1.1.x.x is available in **Provisioned Accounts,** after upgrading to Oracle Identity Manager 11.1.2.2.0. To view, go to the following path:
  1. Connect to the Oracle Identity Manager Identity console.
  2. Go to **Administration**.
  3. Select **Organizations**.
  4. Search for organizations.
  5. Select any organization.
  6. Go to **Provisioned Accounts** to see all Oracle Identity Manager 11.1.1.x.x based resources, provisioned to an organization.
- In Oracle Identity Manager 11.1.1.x.x, data object permission was shown in the Administration Console under **Roles**.

  In Oracle Identity Manager 11.1.2.2.0, data object permission is not shown.
- Oracle Identity Manager 11.1.2.2.0 based Oracle Identity Manager reports is supported in BI Publisher 11g.

11.4.2 Validating the Database Objects

If you are using Oracle Database, you must check for the INVALID schema objects, and compile them if there are any. To do this, complete the following steps:

1. Identify the INVALID schema objects by running the following SQL query as SYS user:

   ```
   SELECT owner,object_type,object_name,status FROM dba_objects WHERE
   status='INVALID' AND owner in ('<OIM_Schema_Name1>') ORDER BY owner,
   object_type, object_name;
   ```

2. If there are any INVALID schema objects, you must compile them by connecting to the database as SYS user, and running the following from SQL*Plus:

   ```
   @<$Oracle_Database_Home_Location>/rdbms/admin/utlrp.sql
   ```

   After running the utlrp.sql, run the SQL query described in step-1 to ensure that there are no INVALID Database objects.

11.4.3 Creating sysadmin Key

After you upgrade OIM 11.1.1.x.x to 11.1.2.2.0, you must manually create the sysadmin key using Oracle Enterprise Manager console. To do this, complete the following steps:

1. Log in to the Oracle Enterprise Manager console using the following URL:

   ```
   http://<host>:<port>/em
   ```

2. Select **Farm_base_domain**.
3. Expand **WebLogic Domain** on the **Target Navigation** pane.
4. Click **base_domain**.
5. Click on the **WebLogic Domain** drop-down list.
6. Click **Security**, and then click **Credentials**.
7. Select **oracle.wsm.security**.
8. Click **Create Key**.
9. Specify the right values for the following fields:
   - **Select Map**: Select **oracle.wsm.security** for this field.
   - ***Key**: Specify **OIMAdmin**.
   - **Type**: Select **Password**.
   - ***User Name**: Specify the username of the system administrator. For example, xelsysadm.
   - ***Password**: Specify the password of the system administrator.
   - ***Confirm Password**: Retype the password to confirm.
10. Click **OK**.

11.4.4 Impact of Removing Approver-Only Attribute in Request Data Set

Removing approver-only attribute in the Request Data Set results in the following:

- Before upgrade: The requester cannot see attributes approver-only='true', during request submission.

  After upgrade: The requester must provide the value during request submission.

- All attributes in the request data sets marked with `required=true` and `approver-only=true` should be marked as `required=false` in the data set.

  Make the required fields mandatory in the approver screen through user interface customization.

- For information about attributes in the request data sets marked with `required=true`, see Section 11.4.11.2, "User Interface Customization for 11.1.1.x.x Mandatory UDF and OOTB Attributes".

- You must manually add LDAP Sync Validation Handler. To do so, complete the following steps:

  1. Export the `EventHandlers.xml` file by running the following WLST offline command:

     On UNIX:

     ```
     exportAccessData("/db/ldapMetadata/EventHandlers.xml")
     ```

     On Windows:

     ```
     exportAccessData("\\db\\ldapMetadata\\EventHandlers.xml")
     ```

  2. Add the following section of the `EventHandlers.xml` by editing the file in a text editor. Save the file:

     ```
     <validation-handler
     class="oracle.iam.ldapsync.impl.eventhandlers.user.UserCommonNameVa
     lidationHandler" entity-type="User" operation="MODIFY"
     name="UserCommonNameValidationHandler" order="1005" sync="TRUE">

     </validation-handler>

     <validation-handler
     class="oracle.iam.ldapsync.impl.eventhandlers.user.UserCommonNameVa
     lidationHandler" entity-type="User" operation="CREATE"
     name="UserCommonNameValidationHandler" order="1005" sync="TRUE">

     </validation-handler>
     ```

  3. Import the `EventHandlers.xml` file by running the following WLST offline command:

     On UNIX:

     ```
     importAccessData("/db/ldapMetadata/EventHandlers.xml")
     ```

     On Windows:

     ```
     importAccessData("\\db\\ldapMetadata\\EventHandlers.xml")
     ```

- You must manually remove the RDN pre-process handler. To do so, complete the following steps:

  1. Export the `EventHandlers.xml` file by running the following WLST offline command:

     On UNIX:

     ```
     exportAccessData("/db/ldapMetadata/EventHandlers.xml")
     ```

     On Windows:

     ```
     exportAccessData("\\db\\ldapMetadata\\EventHandlers.xml")
     ```

  2. Remove the following section of the `EventHandlers.xml` by editing the file in a text editor. Save the file:

```
<action-handler
orch-target="oracle.iam.platform.kernel.vo.EntityOrchestration"
class="oracle.iam.ldapsync.impl.eventhandlers.user.RDNPreProcessHan
dler" entity-type="User" operation="CREATE"
name="CreateUserRDNPreProcessHandler" stage="preprocess"
sync="TRUE" order="10000">

</action-handler>

<action-handler
orch-target="oracle.iam.platform.kernel.vo.EntityOrchestration"
class="oracle.iam.ldapsync.impl.eventhandlers.user.RDNPreProcessHan
dler" entity-type="User"
operation="MODIFY"name="ModifyUserRDNPreProcessHandler"
stage="preprocess" sync="TRUE" order="10000">

</action-handler>
```

3. Import the `EventHandlers.xml` file by running the following WLST offline command:

   On UNIX:

   ```
   importAccessData("/db/ldapMetadata/EventHandlers.xml")
   ```

   On Windows:

   ```
   importAccessData("\\db\\ldapMetadata\\EventHandlers.xml")
   ```

- If you have any custom validation handlers in your environment, ensure that the validation is re-entrant. For more information, see "Writing Custom Validation Event Handlers" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
- If you have any custom user name policy configured in your environment, see "Writing Custom User Name Policy" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* to ensure the following:
  - Use the recommended `oracle.iam.identity.usermgmt.api.UserNameGenerationPolicy` interface to implement policy, instead of using `oracle.iam.identity.usermgmt.api.UserNamePolicy`.
  - Ensure that Custom User Name policy return is the same user login when the approver updates an attribute that does not contribute in generating user login.

11.4.5 Changes to Request API After Upgrading to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0)

As part of Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0) architecture, changes are introduced to `RequestService` and `UnauthenticatedRequestService` APIs in terms of usage and in terms of concepts involved. Request Template concept is no longer part of Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0) and some methods in these APIs are deprecated. Also, `RequestTemplateService` API is completely deprecated.

This section contains the following topics:

- API Methods Deprecated in RequestService
- API Methods Deprecated in UnauthenticatedRequestService
- SELF Request Types Deprecated

- API Methods That Have Changed in Terms of Usage

11.4.5.1 API Methods Deprecated in RequestService

The following is a list of API methods deprecated in `RequestService`:

- `public List<String> getTemplateNames()` throws `RequestServiceException`
- `public RequestModel getModelForTemplate(String templateName)` throws `RequestServiceException`
- `public RequestDataSet getRestrictedDataSet(String templateName, String entityType)` throws `RequestServiceException`
- `public RequestTemplate getTemplate(String templateName)` throws `RequestServiceException`
- `public void updateApproverOnlyData(String reqId, List<RequestBeneficiaryEntity> benEntities, List<RequestEntity> reqEntities)` throws `RequestServiceException`
- `public List<String> getTemplateNamesForSelf()` throws `RequestServiceException`
- `public List<RequestTemplate> getRequestTemplates(RequestTemplateSearchCriteria searchCriteria, Set<String> returnAttrs, Map<String,Object> configParams)` throws `RequestServiceException`

The following is a list of API methods deprecated due to storing comments in SOA Human Task comments feature:

- `public void addRequestComment(String reqId, RequestComment comment)` throws `RequestServiceException`
- `public List<RequestComment> getRequestComments(String reqId)` throws `RequestServiceException`
- `public List<RequestComment> getRequestComments(String reqId, RequestComment.TYPE type)` throws `RequestServiceException`
- `public List<RequestComment> getRequestComments(String reqId, String taskId, RequestComment.TYPE type)` throws `RequestServiceException`

11.4.5.2 API Methods Deprecated in UnauthenticatedRequestService

The following is a list of API methods deprecated in `UnauthenticatedRequestService`:

- `public List<String> getTemplateNames()` throws `RequestServiceException`
- `public RequestTemplate getTemplate(String templateName)` throws `RequestServiceException`
- `public RequestDataSet getRestrictedDataSet(String templateName, String entitySubType)` throws `RequestServiceException`

11.4.5.3 SELF Request Types Deprecated

Request types which were used to perform `SELF` operations have been deprecated. These operations include the following:

- Self Modify User
- Self Assign Roles

- Self Remove Roles
- Self Provision Resource
- Self De-provision Resource
- Self Modify Resource

You can continue with these operations by using the corresponding non-self request types.

11.4.5.4 API Methods That Have Changed in Terms of Usage

The only method that have changes in usage is `RequestService.submitRequest()/UnauthenticatedRequestService.submitRequest()`. The API method signature remains the same. However, the way `RequestData` Value Objects are created, have changed. The changes are covered in the following sections:

- Changes to Entity-Type
- Changes to Value Objects
- Code Examples

11.4.5.4.1 Changes to Entity-Type Changes to entity-type includes the following:

- `Resource` entity-type is replaced with `Application Instance`.

  Beginning from Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0), in order to create any provision, revoke, disable, and enable account type of request, the `entityType` property must be set to `ApplicationInstance` instead of `Resource`.

- A new entity-type called `Entitlement` is introduced in Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0). Oracle Identity Manager supports creating `Provision Entitlement` and `Revoke Entitlement` type of requests.

11.4.5.4.2 Changes to Value Objects Changes to value objects, related to `RequestData` includes the following:

- `requestTemplateName` property which was a part of `oracle.iam.request.vo.RequestData` value objects is deprecated. Even if you set this property, it is not honoured.
- A new property called `operation` is introduced in `oracle.iam.request.vo.RequestEntity` and `oracle.iam.request.vo.RequestBeneficiaryEntity` value objects. It is mandatory to set this property while creating the value objects. You can use the following constants defined in `oracle.iam.request.vo.RequestConstants` class.
  - `MODEL_CREATE_OPERATION` – Create User operation
  - `MODEL_MODIFY_OPERATION` – Modify User operation
  - `MODEL_DELETE_OPERATION` – Delete User operation
  - `MODEL_ENABLE_OPERATION` – Enable User operation
  - `MODEL_DISABLE_OPERATION` – Disable User operation
  - `MODEL_ASSIGN_ROLES_OPERATION` – Assign Roles operation
  - `MODEL_REMOVE_ROLES_OPERATION` – Remove Roles operation
  - `MODEL_PROVISION_APPLICATION_INSTANCE_OPERATION` – Provision Application Instance operation

- MODEL_MODIFY_ACCOUNT_OPERATION – Modify Account operation
- MODEL_REVOKE_ACCOUNT_OPERATION – Revoke Account operation
- MODEL_ENABLE_ACCOUNT_OPERATION – Enable Account operation
- MODEL_DISABLE_ACCOUNT_OPERATION – Disable Account operation
- MODEL_PROVISION_ENTITLEMENT_OPERATION – Provision Entitlement operation
- MODEL_REVOKE_ENTITLEMENT_OPERATION – Revoke Entitlement operation
- MODEL_ACCESS_POLICY_PROVISION_APPINSANCE_OPERATION – Access Policy based provisioning operation

- While creating RequestEntity or RequestBeneficiaryEntity value objects, you can also use the following method to set the entityType property:

  public void setRequestEntityType(oracle.iam.platform.utils.vo.OIMType type)

  type - OIMType.Role/ OIMType.ApplicationInstance/OIMType.Entitlement/ OIMType.User

11.4.5.4.3 Code Examples Listed below are some code examples:

- Create a RequestData for a Create User operation as follows:

```
RequestData requestData = new RequestData("Create User");
requestData.setJustification("Creating User John Doe");
String usr = "John Doe";

RequestEntity ent = new RequestEntity();
ent.setEntityType(RequestConstants.USER);
ent.setOperation(RequestConstants.MODEL_CREATE_OPERATION); //New in R2
List<RequestEntityAttribute> attrs = new ArrayList<RequestEntityAttribute>();

RequestEntityAttribute attr = new RequestEntityAttribute("Last Name", usr,
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
attr = new RequestEntityAttribute("First Name", usr,
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
attr = new RequestEntityAttribute("User Login", usr,
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
attr = new RequestEntityAttribute("Password", "Welcome123",
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
attr = new RequestEntityAttribute("Organization", 1L,
RequestEntityAttribute.TYPE.Long);
attrs.add(attr);
attr = new RequestEntityAttribute("User Type", false,
RequestEntityAttribute.TYPE.Boolean);
attrs.add(attr);
attr = new RequestEntityAttribute("Role", "Full-Time",
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
ent.setEntityData(attrs);

List<RequestEntity> entities = new ArrayList<RequestEntity>();
entities.add(ent);
requestData.setTargetEntities(entities);
```

```
//Submit the request with the above requestData
```

- Create a `RequestData` for an Assign Roles operation as follows:

```
RequestData requestData = new RequestData();

requestData.setJustification("Assigning IDC ADMIN Role(role key 201) to user
with key 121");

RequestBeneficiaryEntity ent1 = new RequestBeneficiaryEntity();
ent1. setRequestEntityType (oracle.iam.platform.utils.vo.OIMType.Role);
ent1.setOperation(oracle.iam.request.vo.RequestConstants.MODEL_ASSIGN_ROLES_
OPERATION); //New in R2
ent1.setEntitySubType("IDC ADMIN");
ent1.setEntityKey("201");

List<RequestBeneficiaryEntity> entities = new
ArrayList<RequestBeneficiaryEntity>();
entities.add(ent1);

Beneficiary beneficiary = new Beneficiary();
beneficiary.setBeneficiaryKey("121");
beneficiary.setBeneficiaryType (Beneficiary.USER_BENEFICIARY);
beneficiary.setTargetEntities(entities);

List<Beneficiary> beneficiaries = new ArrayList<Beneficiary>();
beneficiaries.add(beneficiary);
requestData.setBeneficiaries(beneficiaries);

//Submit the request with the above requestData
```

- Create a `RequestData` for a Provision Application Instance operation as follows:

```
RequestData requestData = new RequestData();

requestData.setJustification("Creating AD User (app instance key 201) account
to user with key 121");

RequestBeneficiaryEntity ent1 = new RequestBeneficiaryEntity();
ent1. setRequestEntityType
(oracle.iam.platform.utils.vo.OIMType.ApplicationInstance);
ent1.setOperation(oracle.iam.request.vo.RequestConstants.MODEL_PROVISION_
APPLICATION_INSTANCE_OPERATION);
ent1.setEntitySubType("AD User");
ent1.setEntityKey("201");

List<RequestBeneficiaryEntityAttribute> attrs = new
ArrayList<RequestBeneficiaryEntityAttribute>();
//Update 'attrs' above with all the data specific to AD User form.
ent1.setEntityData(attrs);

List<RequestBeneficiaryEntity> entities = new
ArrayList<RequestBeneficiaryEntity>();
entities.add(ent1);

Beneficiary beneficiary = new Beneficiary();
beneficiary.setBeneficiaryKey("121");
beneficiary.setBeneficiaryType(Beneficiary.USER_BENEFICIARY);
beneficiary.setTargetEntities(entities);

List<Beneficiary> beneficiaries = new ArrayList<Beneficiary>();
```

```
beneficiaries.add(beneficiary);
requestData.setBeneficiaries(beneficiaries);
//Submit the request with the above requestData
```

- Create a `RequestData` for a Provision Entitlement operation as follows:

```
RequestData requestData = new RequestData();
Beneficiary beneficiary1 = new Beneficiary();
beneficiary1.setBeneficiaryKey("222");
beneficiary1.setBeneficiaryType(Beneficiary.USER_BENEFICIARY);

RequestBeneficiaryEntity ent1 = new RequestBeneficiaryEntity();
ent1.setEntityType(RequestConstants.ENTITLEMENT);
ent1.setEntitySubType("AD USER ENTITLEMENT1");
ent1.setEntityKey("122");
ent1.setOperation(RequestConstants.MODEL_PROVISION_ENTITLEMENT_OPERATION);

List<RequestBeneficiaryEntity> entities1 = new
ArrayList<RequestBeneficiaryEntity>();
entities1.add(ent1);
beneficiary1.setTargetEntities(entities1);

List<Beneficiary> beneficiaries = new ArrayList<Beneficiary>();
beneficiaries.add(beneficiary1);
requestData.setBeneficiaries(beneficiaries);
//Submit the request with the above requestData
```

11.4.6 Enabling Oracle Identity Manager-Oracle Access Manager Integration After Upgrading to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0)

> **Note:** Perform this task only if you want to integrate Oracle Identity Manager with Oracle Access Manager for single sign-on, after upgrading to Oracle Identity Manager 11.1.2.2.0.
>
> Ensure that Oracle Access Manager is at release 11.1.1.5.2 or later.

If you want to integrate Oracle Identity Manager 11.1.2.2.0 with Oracle Access Manager for single sign-on, then you must upgrade Oracle Access Manager to 11.1.1.5.2 or later. If your Oracle Access Manager version is less than 11.1.1.5.2, the auto-login functionality does not work.

After upgrading to Oracle Identity Manager 11.1.2.2.0, upgrade Oracle Identity Manager and Oracle Access Manager configurations for auto-login functionality to work. After upgrading the configurations, NAP protocol is replaced by TAP protocol for communication between Oracle Identity Manager and Oracle Access Manager.

The following topics provide upgrade instructions for two possible scenarios:

- Using 10g WebGate for Oracle Identity Manager-Oracle Access Manager Integration
- Using 11g WebGate for Oracle Identity Manager-Oracle Access Manager Integration

Before you begin with the upgrade configuration procedures, refer to the "Using the idmConfigTool Command" for more about the **IdmConfigTool** in the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

11.4.6.1 Using 10*g* WebGate for Oracle Identity Manager-Oracle Access Manager Integration

If you are using 10*g* WebGate, complete the following steps to upgrade Oracle Identity Manager and Oracle Access Manager configurations:

1. In the **idmConfigTool**, run `configOAM`. This creates a 10*g* WebGate agent and an 11*g* WebGate agent in Oracle Access Manager. Ensure that the artifacts corresponding to both WebGates are created in `<DOMAIN_HOME>/output directory`.
2. In the **idmConfigTool**, run `configOIM`. In a cross-domain setup where Oracle Identity Manager and Oracle Access Manager are in two different WebLogic domains, specify the following additional properties before running this option:
   - `OAM11G_WLS_ADMIN_HOST: <host name of OAM admin server machine>`
   - `OAM11G_WLS_ADMIN_PORT: <OAM admin server port>`
   - `OAM11G_WLS_ADMIN_USER: <admin user of OAM domain>`

   Note: When running the `configOIM` option, ensure that you provide the same properties that you provided in the `configOAM` option for `OAM_TRANSFER_MODE` and `ACCESS_GATE_ID` properties.

   The `WEBGATE_TYPE` property should be specified as `ohsWebgate10g`.
3. Restart the Administration and Managed Servers. In the case of a cross domain setup, restart servers from both the domains.

   Restart the Oracle Identity Manager Administration Server and Managed server as follows:

   On UNIX:

   ```
   <MW_HOME>/user_projects/domains/domain_name/startWebLogic.sh

   <MW_HOME>/user_projects/domains/domain_
   name/bin/startManagedWebLogic.sh <managed_server1>
   ```

   On Windows:

   ```
   <MW_HOME>\user_projects\domains\domain_name\startWebLogic.cmd

   MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd
   <oim_server>
   ```

   For more information, see "Restarting Servers" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

11.4.6.2 Using 11*g* WebGate for Oracle Identity Manager-Oracle Access Manager Integration

If you are using 11*g* WebGate, complete the following steps to upgrade Oracle Identity Manager and Oracle Access Manager configurations:

1. In the **idmConfigTool**, run `configOAM`. This creates a 10*g* WebGate agent and an 11*g* WebGate agent in Oracle Access Manager. Ensure that the artifacts corresponding to both WebGates are created in the `<DOMAIN_HOME>/output directory`.

2. In the **idmConfigTool**, run `configOIM`. In cross-domain setup where Oracle Identity Manager and Oracle Access Manager are in two different WebLogic domains, specify the following additional properties before running this option:
   - `OAM11G_WLS_ADMIN_HOST: <host name of OAM admin server machine>`
   - `OAM11G_WLS_ADMIN_PORT: <OAM admin server port>`
   - `OAM11G_WLS_ADMIN_USER: <admin user of OAM domain>`

   Note: When running the `configOIM` option, ensure that you provide the same properties that you provided in the `configOAM` option for `OAM_TRANSFER_MODE` and `ACCESS_GATE_ID` properties.

   The `WEBGATE_TYPE` property should be specified as `ohsWebgate11g`.

3. Restart the Administration and Managed servers. In the case of a cross domain setup, restart servers from both the domains.

   Restart the Oracle Identity Manager Administration Server and Managed server as follows:

   On UNIX:

   ```
   <MW_HOME>/user_projects/domains/domain_name/startWebLogic.sh
   ```

   ```
   <MW_HOME>/user_projects/domains/domain_
   name/bin/startManagedWebLogic.sh <managed_server1>
   ```

   On Windows:

   ```
   <MW_HOME>\user_projects\domains\domain_name\startWebLogic.cmd
   ```

   ```
   MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd
   <oim_server>
   ```

   For more information, see "Restarting Servers" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

11.4.7 Running the Entitlement List Schedule

You must run the Entitlement List Schedule task in order to use catalog features.

Complete the following steps to run the Entitlement List Schedule job:

1. Log in to the following location:

   ```
   http://<OIM_HOST>:<OIM_PORT>/sysadmin
   ```

2. Click **System Management**.
3. Select **Scheduler**.
4. Enter "Entitlement List" in the **Search Scheduled Jobs** field and click **Search**.
5. Select **Entitlement List**.
6. Click **Run Now**. Wait till the job is complete.

11.4.8 Running the Evaluate User Policies Scheduled Task

You must run the Evaluate User Policies scheduled task to start provisioning based on access policy after the role grant. This scheduled task can be configured to run every 10 minutes, or you can run this scheduled task manually.

To start the scheduler, see "Starting and Stopping the Scheduler" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

11.4.9 Running Catalog Synchronization

Resource objects are transformed during the upgrade process. In order to provision the resource of an object, called App instance, with Oracle Identity Manager 11.1.2.2.0, you must run the Catalog Synchronization job.

For more information, see "Bootstrapping the Catalog" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

Note: If no Entitlements show up, make sure that the entitlements field in the child tables is set to `Entitlement=true` and reloaded into the parent form.

11.4.10 UMS Notification Provider

This is a new Oracle Identity Manager 11.1.2.2.0 feature for notification. If you want to use this new notification model, after upgrading to 11.1.2.2.0, complete the following steps:

1. Configure E-mail driver from Enterprise Manager user interface:
   a. Log in to Oracle Enterprise Manager Fusion Middleware Control and do the following:

      i. Expand **Application Deployments**.

      ii. Expand **User Messaging Service**.

      iii. Select **usermessagingdriver-email (<soa_server1>)**.

      iv. Select **Email Driver Properties**.

      v. Select **in Driver-Specific Configuration**.

   b. Configure the values, as listed in Table 11–15:

Table 11–15 UMS Parameters and Description

Parameter	Description
OutgoingMailServer	Name of the SMTP server. For example: `abc.example.com`
OutgoingMailServerPort	Port of the SMTP server. For example: 456
OutgoingMailServerSecurity	The security setting used by the SMTP server Possible values can be None/TLS/SSL.
OutgoingUsername	Provide a valid username. For example: `abc.eg@example.com`

Table 11–15 (Cont.) UMS Parameters and Description

Parameter	Description
OutgoingPassword	Complete the following: 1. Select **Indirect Password**. Create a new user. 2. Provide a unique string for indirect **Username/Key**. For example: `OIMEmailConfig`. This mask the password and prevent it from exposing it in cleartext, in the config file. 3. Provide valid password for this account.

2. Configure the Notification provider XML through the Enterprise Manager user interface:
   a. Log in to Enterprise Manager and do the following:
      i. Expand **Application Deployments**.
      ii. Select **OIMAppMetadata(11.1.1.3.0)(oim_server1)** and right-click.
      iii. Select **System MBean Browser**.
      iv. Expand **Application Defined MBeans**.
      v. Expand **oracle.iam**.
      vi. Expand **Server_OIM_Server1**
      vii. Expand **Application: oim**.
      viii. Expand **IAMAppRuntimeMBean**.
      ix. Select **UMSEmailNotificationProviderMBean**.
   b. Configure the values, as listed in Table 11–16:

Table 11–16 Parameter for Configuring Notification Provider

Parameter	Description
Web service URL	Start the URL of UMS web service. Any SOA server can be used. For example: `http://<SOA_host>:<SOA_Port>/ucs/messaging/webservice`
Policies	The OWSM Policy is attached to the given web service, leave it blank.
Username	The username is given in the security header of web service. If there is no policy attached, leave it blank.
Password	The password given in the security header of web service. If there is no policy attached, leave it blank.

After upgrading to 11.1.2.2.0, if you want to use SMTP notification provider instead of the default UMS notification provider, do the following:

1. Log in to Enterprise Manager and do the following:
   a. Expand **Application Deployments**.
   b. Select **OIMAppMetadata(11.1.1.3.0)(oim_server1)** and Right click.
   c. Select **System MBean Browser**.

d. Expand **Application Defined MBeans**.

e. Expand **oracle.iam**.

f. Expand **Server_OIM_Server1**

g. Expand **Application: oim**.

h. Expand **IAMAppRuntimeMBean**.

i. Select **UMSEmailNotificationProviderMBean**.

2. Ensure that the value of the attribute `Enabled` is set to `true`.

3. Provide the configuration values in MBean (username, password, mailServerName) or the name of IT Resource in MBean.

   The IT Resource name is the name given in `XL.MailServer` system property, before you upgrade Oracle Identity Manager 11.1.1.x.x to Oracle Identity Manager 11.1.2.2.0.

11.4.11 Upgrading User UDF

You must have UDF in your environment because if you do not update your User Interface with UDFs, several features like user creation, role creation, and self registration request where UDFs are involved fails.

This section contains the following topics:

- Rendering the UDFs
- User Interface Customization for 11.1.1.x.x Mandatory UDF and OOTB Attributes
- Lookup Query Modification

11.4.11.1 Rendering the UDFs

For an Oracle Identity Manager 11.1.2.2.0 environment that has been upgraded from Oracle Identity Manager 11.1.1.x.x, the custom attributes for user entity already exist in the back-end. These attributes are not present as form fields on the Oracle Identity Manager 11.1.2.2.0 user interface screens until the user screens are customized to add the custom fields.

However, before you can customize the screens, you must first complete upgrading the custom attributes using the Upgrade User Form link in the System Administration console.

After completing the Upgrade User Form, the User value object (VO) instances in various Data Components like DataComponent-Catalog, DataComponent-My Information, DataComponent-User Registration shows the custom attributes. This includes all custom attributes available for Web Composer (Customized) and can be added to User user interface screens.

For more information, see "Customizing the Interface" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Complete the following steps to render UDFs:

1. Log in to the **Identity System Administration** console.

2. Click **Sandboxes**. Click **Create Sandbox**. A Create Sandbox window appears.

3. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.

4. Go to **Upgrade**. Select **Upgrade User Form**. Click **Upgrade Now**.

Note: If an error message is displayed after clicking `Upgrade Now` button, it is important that you analyze the error. You must also export the Sandbox for analysis and then discard (Delete) the sandbox. This note also applies to `Upgrade Role Form` and `Upgrade Organization Form`.

5. Publish the Sandbox.
6. Log out from Identity System Administration console.
7. Log in to **Identity Self Service** console.
8. Click **Create Sandbox**. A **Create Sandbox** window appears.
9. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
10. From the left navigation pane, select **Users**.
11. Click **Create User**. A **Create User** page opens. Fill up all the mandatory fields. Add the same UDFs in **Modify User** and **User Detail** screen. Select the correct **Data Component** and **UserVO Name** as listed in Table 11–17.

    For example:

    From the left navigation pane, click **Users**. Click **User** to go to the **Create User** screen and fill all mandatory fields.
12. Click **Customize** on top right. Select **View**. Select **Source**.
13. Select **Name** in **Basic Information** and click **Edit** on the confirmation window.
14. Select **panelFormLayout**. Click **Add Content**.
15. Select the correct **Data Component** and **VO Name** as listed in Table 11–17:

Table 11–17 UDF Screens and Description

Screen Name	Data Component	VO Name	Procedure
Create User	Data Component - Catalog	UserVO	Do the following: 1. Click **User**. 2. Click **Create**, it launches the **Create User** screen.
Modify User	Data Component - Catalog	UserVO	Do the following: 1. Click **User** and search. 2. Select a single user from search results. 3. Click **Edit**, it launches the **Modify User** screen.
View User Details	Data Component - Manage Users	UserVO1	Do the following: 1. Click **User** and search. 2. Select a single user from search results.
Bulk Modify User Flow	Data Component - Catalog	UserVO	Do the following: 1. Click **User** and search. 2. Select more than a single user from search results.

Table 11–17 (Cont.) UDF Screens and Description

Screen Name	Data Component	VO Name	Procedure
My Information	Data Component - My Information	UserVO1	Do the following: 1. Click **Identity**. 2. Select the **My Information** sub-tab.
Customizing Search Results	Data Component - Manage Users	UserVO1	Do the following: 1. Click **Identity**. 2. Click **Users**. 3. Click **Customizations**, it opens the **Web Composer**.
User Registration	Data Component - User Registration	UserVO1	Do the following: 1. Click **Customize** to open **Web Composer**. 2. Enable the left navigation links for unauthenticated pages. 3. Click **User Registration**. 4. Select **User Registration**.
Adding UDF in Search Panel	NA	NA	Do the following: 1. Log in to Identity 2. Click **User**. 3. Search for "Add Fields" in the search box. It shows all searchable fields to the user.
Customizing Request Summary/Details	NA	NA	Requests created after Create User, Modify User, My Information, Self Registration.

16. Click **Close**.
17. Click **Sandboxes**. Export the sandbox using **Export Sandbox.**
18. Publish the sandbox.
19. Log out from **Identity Self Service**, and log in again. The added UDF in the screen is seen.

> **Note:** You can upgrade and customize Role UDF and Organization UDF by following the instructions described in the table "Entities and Corresponding Data Components and View Objects" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

11.4.11.2 User Interface Customization for 11.1.1.x.x Mandatory UDF and OOTB Attributes

If you have rendered the OOTB attributes as mandatory in Oracle Identity Manager 11.1.1.x.x, you must customize the user interface in order to achieve the same customizations after upgrade.

1. Log in to **Identity System Administration** console.

2. Click **Sandboxes**. Click **Create Sandbox**. A Create Sandbox window appears.
3. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
4. Go to **Upgrade**. Select **Upgrade User Form**. Click **Upgrade Now**.
5. Publish the Sandbox.
6. Log out from Identity System Administration console.
7. Log in to **Identity Self Service** console.
8. Click **Create Sandbox**. A **Create Sandbox** window appears.
9. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
10. From the left navigation pane, click **Users**. Click **User** to go to the **Create User** screen and fill all the mandatory fields.
11. Click **Customize** on top right. Select **View**. Select **Source**.
12. Select **Name** in **Basic Information** and click **Edit** on the confirmation window.
13. Select **panelFormLayout**. Click **Add Content**.
14. Click **Input Component** and click **Edit**.
15. On the Component Properties dialogue, select **Show Required** check box. In the Required field, select **Expression Editor**, and in the **Expression Editor** field, enter the value as **true**.
16. Click **Close**.
17. Click **Sandboxes**. Export the sandbox using **Export Sandbox.**
18. Publish the sandbox.
19. Log out from **Identity Self Service**, and log in again. The added UDF on the screen with an asterix (*) symbol is seen.

11.4.11.3 Lookup Query Modification

In user customization upgrade, multiple values for the Save Column may exist in `User.xml`. Based on the possible values; single, multiple, and null, do the following in the upgraded environment:

- Use `Single` value for Save Column: User creation is successful, and the value of the field is also saved in database.
- Use `Multiple` or `NULL` value for Save Column: User creation is successful, but the value is not saved in database.

Recommendation

Update the **Lookup By Query** metadata definition attached to an attribute in User or Role through Config Service or Design Console.

For more information, see Section 11.3.16, "Upgrading Oracle Identity Manager Design Console".

11.4.12 Upgrading Application Instances

After you complete the upgrade, you must complete the following steps to upgrade Application Instances:

1. Log in to the following console:

`http://<OIM_HOST>:<OIM_PORT>/sysadmin`

2. Expand **Upgrade** on the left navigation pane.
3. Click **Upgrade Application Instances**.

This creates the U/I Forms and Datasets for the Application Instances, and seeds to MDS.

11.4.13 Redeploying XIMDD

> **Note:** This section is required only if the Diagnostic Dashboard services for AD Password Sync were deployed in 11.1.1.x.x and if your application is deployed in staging mode in 11.1.1.x.x.

Before you can re-deploy, you must undeploy XIMDD from the 11.1.1.x.x Oracle Identity Manager Managed Server or from the cluster. To do so, complete the following steps:

1. Log in to the WebLogic Server Administration console:

   `host:admin port/console`
2. If you are running in production mode, click **Lock and Edit**.
3. Click **Deployments**.
4. In the resulting list, look for **XIMDD**.
5. If they are running, select **XIMDD.**
6. Click **Delete**.
7. Activate the changes.

To redeploy, complete the following steps:

1. Log in to the WebLogic Server Administration console:

   `host:admin port/console`
2. Click **Lock & Edit**.
3. Click **Deployments**.
4. Click **Install**.
5. In the path, provide the path for XIMDD.ear.

   The default path is in the following location:

   On UNIX, `$<OIM_HOME>/server/webapp/optional`

   On Windows, `<OIM_HOME>\server\webapp\optional`
6. Select **XIMDD.ear**. Click **Next**.
7. Select **Install this deployment as an application**. Click **Next**.
8. In **Select deployment targets** page, select **oim server**. Click **Next**.
9. In the **Optional Setting** page, click **Finish**.
10. Click **Deployments**.
11. Select **XIMDD**. Click **Start**.

12. From the options, select **Service All Requests**.

11.4.14 Redeploying SPML-DSML

> **Note:** This section is required only if the DSML web services for AD Password Sync were deployed in 11.1.1.x.x.

Before you can redeploy, you must undeploy SPML-DSML from the 11.1.1.x.x Oracle Identity Manager Managed Server or from the cluster. To do so, complete the following steps:

1. Log in to the WebLogic Server Administration console:

   `host:admin port/console`

2. If you are running in production mode, obtain the Lock in order to make updates.
3. Click **Deployments**.
4. In the resulting list, look for **spml**.
5. If they are running, select **spml.**
6. Click **Delete**.
7. Activate the changes.

To redeploy, complete the following steps:

1. Log in to WebLogic Server Administration console through the following path:

   `host:admin port/console`

2. Click **Lock & Edit**.
3. Click **Deployments**.
4. Click **Install**.
5. In the path provide the path for spml.ear.

   The default path is in the following location:

   On UNIX, `$<OIM_HOME>/server/apps`

   On Windows, `<OIM_HOME>\server\apps`

6. Select **spml-dsml.ear**. Click **Next**.
7. Select **Install this deployment as an application**. Click **Next**.
8. In **Select deployment targets** page, select **oim server**. Click **Next**.
9. In the **Optional Setting** page, click **Finish**.
10. Click **Deployments**.
11. Select **spml**. Click **Start**.
12. From the options, select **Service All Requests**.

11.4.15 Customizing Event Handlers

If you have used any event handlers in Oracle Identity Manager 11.1.1.x.x, you must re-customize the event handler for Oracle Identity Manager 11.1.2.2.0.

For more information, see "Developing Custom Event Handlers" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

11.4.16 Upgrading SOA Composites

You must manually upgrade OOTB composites and custom composites built before upgrading to 11.1.2.2.0.

This section contains the following topics:

- OOTB Composites Not Modified Before Upgrading
- OOTB Composites Modified Before Upgrading And Custom Composites

Note: Redeploying a composite moves all pending tasks to `STALE` state. Oracle recommends you to close any pending task before upgrading the composites.

11.4.16.1 OOTB Composites Not Modified Before Upgrading

Upgrade OOTB composites that are not modified, using either JDeveloper or SOA Composer, before upgrading to Oracle Identity Manager 11.1.2.2.0. Complete the following steps to upgrade `DefaultRequestApproval` composite:

1. Move from your present working directory to the `<OIM_ORACLE_HOME>/server/workflows` directory by running the following command on the command line:

   On UNIX:

   ```
   cd <OIM_ORACLE_HOME>/server/workflows
   ```

   On Windows:

   ```
   cd <OIM_ORACLE_HOME>\server\workflows
   ```

2. Unzip `DefaultRequestApproval.zip`.
3. Log in to the Oracle Enterprise Manager console:

   ```
   http://<host>:<port>/em
   ```

4. Expand **Farm_<oim_domain_name>_d > SOA -> soa-infra -> default**.
5. Right click **DefaultRequestApproval[1.0]** and select **SOA Deployment -> Redeploy**.
6. Select **Archive is on the machine where Enterprise Manager is running**.
7. Provide the absolute path to the `sca` jar for `DefaultRequestApproval` composite:

   On UNIX:

   ```
   <OIM_
   HOME>/server/workflows/composites/DefaultRequestApproval/deploy/sca_
   DefaultRequestApproval_rev1.0.jar
   ```

   On Windows:

   ```
   <OIM_
   HOME>server\workflows\composites\DefaultRequestApproval\deploy\sca_
   DefaultRequestApproval_rev1.0.jar
   ```

8. Select **No Configuration plan is required**.

9. Click **Next**.
10. Select **Deploy as default revision**.
11. Click **Redeploy**.

Repeat steps 2 to 11 for the remaining composites, which were not modified before upgrading to Oracle Identity Manager 11.1.2.2.0.

Note: `DefaultResourceAuthorizer` and `DefaultResourceAdministrator` are no longer supported in 11.1.2.2.0.

11.4.16.2 OOTB Composites Modified Before Upgrading And Custom Composites

Upgrade custom composites created before upgrading to Oracle Identity Manager 11.1.2.2.0 and OOTB composites modified, using either JDeveloper or SOA Composer, before upgrading to Oracle Identity Manager 11.1.2.2.0. Complete the following steps to upgrade `DefaultRequestApproval` composite:

1. Open the SOA composite project in JDeveloper (Use Jdeveloper 11.1.1.6.0).
2. Open `ApprovalTask.task` file in designer mode.
3. Select **General**.
4. Change **Owner** to **Group, SYSTEM ADMINISTRATORS, STATIC**.
5. Select **Outcomes lookup**. An **Outcomes Dialog** opens.
6. Select **Outcomes Requiring Comment**.
7. Select **Reject** and click **Ok**.
8. Click **Ok** again.
9. Select **Notification**.
10. Click on the update icon under **Notification**. Update any old URLs in notification with the corresponding new URL in 11.1.2.2.0. An example notification content is given below:

```
A <%/task:task/task:payload/task:RequestModel%> request has been assigned to
you for approval. <BR><BR>
Request ID: <%/task:task/task:payload/task:RequestID%> <BR>
Request type: <%/task:task/task:payload/task:RequestModel%> <BR>
<BR>
Access this task in the
<A
style="text-decoration: none;"
href=<%substring-before(/task:task/task:payload/task:url,
"/workflowservice/CallbackService")%>/identity/faces/home?tf=approval_details
>
Identity Self Service
</A>
 application or take direct action using the links below. Approvers are
required to provide a justification when rejecting the request
```

11. Click **Advanced**.
12. Deselect **Show worklist/workspace URL in notifications**. Provide the URL to Pending Approvals in identity application as shown in the example in step 10.
13. Repeat step 1 to 12 for other human tasks, if any, in the composite. Save your work.

14. Right click **Project** and select **Deploy -> Deploy to Application Server**.
15. Provide revision ID. Select **Mark revision as default** and **Overwrite any existing composite with same revision ID**.

    Note: You can also deploy the composites with different revision ID. In that case you have to modify all approval policies using this composite.

16. Select your application server connection, if it already exists, and click **Next**. Create an application server connection if it does not exist.
17. Click **Next**.
18. Click **Finish**.

Repeat the procedure for the remaining custom composites and modified OOTB composites as well.

11.4.17 Provisioning Oracle Identity Management Login Modules Under WebLogic Server Library Directory

Note: This task is required only if `OIMAuthenticator.jar` is already present under the `<MW_HOME>/wlserver_10.3/server/lib/mbeantypes` directory.

Apply the following steps across all the WebLogic Server homes in the domain:

On UNIX:

1. Copy `OIMAuthenticator.jar`, `oimmbean.jar`, `oimsigmbean.jar`, and `oimsignaturembean.jar` files located under `<OIM_ORACLE_HOME>/server/loginmodule/wls` directory to `<MW_HOME>/wlserver_10.3/server/lib/mbeantypes` directory by running the following command on the command line:

   ```
   cp <OIM_ORACLE_HOME>/server/loginmodule/wls/* <MW_HOME>/wlserver_10.3/server/lib/mbeantypes/
   ```

2. Move from your present working directory to the `<MW_HOME>/wlserver_10.3/server/lib/mbeantypes` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/wlserver_10.3/server/lib/mbeantypes
   ```

3. Change the permissions on these files to 750 by using the `chmod` command:

   ```
   chmod 750 *
   ```

4. Restart all servers in the domain.

On Windows:

1. Copy `OIMAuthenticator.jar`, `oimmbean.jar`, `oimsigmbean.jar`, and `oimsignaturembean.jar` files located under `<OIM_ORACLE_HOME>\server\loginmodule\wls` directory to `<MW_HOME>\wlserver_10.3\server\lib\mbeantypes` directory by running the following command on the command line:

```
cp <OIM_ORACLE_HOME>\server\loginmodule\wls\* <MW_HOME>\wlserver_
10.3\server\lib\mbeantypes
```

2. Move from your present working directory to the `<MW_HOME>\wlserver_10.3\server\lib\mbeantypes` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\wlserver_10.3\server\lib\mbeantypes
   ```

3. Change the permissions on these files to 750 by using the `chmod` command:

   ```
   chmod 750 *
   ```

4. Restart all servers in the domain.

11.4.18 Reviewing Performance Tuning Recommendations

After you upgrade to Oracle Identity Manager 11.1.2.2.0, you must review the Oracle Identity Manager specific performance tuning recommendations described in "Oracle Identity Manager Performance Tuning" in the *Oracle Fusion Middleware Performance and Tuning Guide*.

11.4.19 Authorization Policy Changes

If you have custom Authorization Policies in Oracle Identity Manager in 11*g* Release 1 (11.1.1.5.0), in order to create or modify users, you must assign new administrator roles in relation to User Administration, Role Administration, or Help Desk.

Table 11–18 lists the Administration roles in Oracle Identity Manager 11g, either removed or consolidated into the System Administrator Administration role for all system administrative operations in Oracle Identity Manager 11.1.2.2.0:

Table 11–18 Changes in Role from Oracle Identity Manager 11g to 11.1.2.2.0

Sl No.	Roles in Oracle Identity Manager 11*g*	Roles Removed and Replaced in Oracle Identity Manager 11.1.2.2.0
1	SCHEDULER ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
2	DEPLOYMENT MANAGER ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
3	NOTIFICATION TEMPLATE ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
4	SOD ADMINISTRATORS	Removed and replaced with SYSTEM ADMINISTRATORS.
5	SYSTEM CONFIGURATION ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
6	GENERATE_USERNAME_ROLE	Removed and replaced with SYSTEM ADMINISTRATORS.
7	IDENTITY USER ADMINISTRATORS	Removed and replaced with USER ADMIN.
8	USER CONFIGURATION ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
9	ACCESS POLICY ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
10	RECONCILIATION ADMINISTRATORS	Removed and replaced with SYSTEM ADMINISTRATORS.

Table 11–18 (Cont.) Changes in Role from Oracle Identity Manager 11g to 11.1.2.2.0

Sl No.	Roles in Oracle Identity Manager 11*g*	Roles Removed and Replaced in Oracle Identity Manager 11.1.2.2.0
11	RESOURCE ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
12	GENERIC CONNECTOR ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
13	APPROVAL POLICY ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
14	REQUEST ADMINISTRATORS	Removed and replaced with SYSTEM ADMINISTRATORS.
15	REQUEST TEMPLATE ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
16	PLUGIN ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
17	ATTESTATION CONFIGURATION ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
18	ATTESTATION EVENT ADMINISTRATORS	Removed and replaced with SYSTEM ADMINISTRATORS.
19	ROLE ADMINISTRATORS	Removed and replaced with ROLE ADMIN.
20	USER NAME ADMINISTRATOR	Removed and now depends on administration roles.
21	IDENTITY ORGANIZATION ADMINISTRATORS	Removed and replaced with ORGANIZATION ADMIN.
22	IT RESOURCE ADMINISTRATORS	Removed and replaced with APPLICATION INSTANCE ADMIN.
23	REPORT ADMINISTRATORS	No link to reports from Oracle Identity Manager.
24	SPML_APP_ROLE	There is no change in this enterprise role and a corresponding role with the privileges is seeded in Oracle Entitlements Server.
25	ALL USERS	This is an enterprise role, not an administrator role.
26	SYSTEM CONFIGURATORS	All privileges as System Administrator role, except for the ability to manage Users, Roles, Organizations and Provisioning remains unchanged.
27	SYSTEM ADMINISTRATORS	Remains unchanged.

11.4.20 Creating Password Policies

When you upgrade Oracle Identity Manager 11.1.1.x.x to 11.1.2.2.0, a default password policy will be seeded at the TOP organization. As a result, any password policy rules created using the older password policy model in Oracle Identity Manager 11.1.1.x.x environment will not be supported. The upgrade utility does not migrate the password policies of Oracle Identity Manager 11.1.1.x.x to 11.1.2.2.0. If you had made any password policy customizations on the older password policy rules, you must create equivalent password policies using the newer password policy model, and attach it to the respective organization.

For information about creating password policies, see "Managing Password Policies" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

11.4.21 Creating PeopleSoft Enterprise HRMS Reconciliation Profile

If you are upgrading Oracle Identity Manager 11.1.1.x.x with PeopleSoft connector to Oracle Identity Manager 11.1.2.2.0, you must create PeopleSoft HRMS reconciliation profile after you upgrade to 11.1.2.2.0. For information about creating reconciliation profile, see "Updating Reconciliation Profiles Manually" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

11.4.22 Reviewing OIM Data Purge Job Parameters

This post-upgrade task is optional.

While upgrading Oracle Identity Manager to 11.1.2.2.0, the `OIM Data Purge Job` will be seeded in `enabled` state. By default, it will purge platform data with a retention period of 1 day for complete orchestration. To enable purge of request, reconciliation, and provisioning task, you must revisit the `OIM Data Purge Job` parameters.

For information about the user-configurable attributes, see "Configuring Real-Time Purge and Archival" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

11.4.23 Migrating Customized Oracle Identity Manager Reports

For customized reports built on any version of Oracle BI Publisher between 11*g* Release 1 (11.1.1.5.0) and 11*g* Release 1 (11.1.1.6.4), you do not need to upgrade the custom reports. You can export your customized reports from your existing report repository and import the reports into your new 11.1.1.7.1 repository.

Customized reports built on Oracle BI Publisher 10*g* Release 3 (10.1.3.X) or later must be upgraded before they can be consumed by Oracle BI Publisher 11.1.1.7.1. You must use the Upgrade Assistant to upgrade the reports in the BI Publisher 10g repository. For more information, see "Task 5: Upgrade the BI Publisher Repository" in the *Oracle Fusion Middleware Upgrade Guide for Oracle Business Intelligence*.

11.4.24 Reviewing Connector Certification

Before you upgrade your existing Oracle Identity Manager environments, you must verify if the version of the existing connector is supported for Oracle Identity Manager 11.1.2.2.0. For information about the supported connector versions for Oracle Identity Manager 11.1.2.2.0, refer to the sections "Certified Components" and "Usage Recommendation" in the respective *Connector Guide* in Oracle Identity Manager Identity Connectors Documentation Library.

If you are using 9.x connector or GTC connector, do the following:

- If the 9.x connector that you are using is supported, you can continue to use the existing connector.
- If the 9.x connector is not supported, you must upgrade the existing 9.x connector to the latest 11.x connector after you upgrade the Oracle Identity Manager server to 11.1.2.2.0.
- Verify the data in the `Lookup` populated through lookup reconciliation that the IT Resource Key & IT Resource name is pre-fixed for code & decode respectively. If not, you must upgrade the existing connector to the latest available connector after you upgrade Oracle Identity Manager server.

If you are using 11g connector, the connector upgrade is not required.

11.4.25 Verifying the Functionality of Connectors

After you upgrade Oracle Identity Manager to 11.1.2.2.0, complete the following steps to verify the functionality of connectors:

- Verify if Account and Entitlement Tagging are available on the process form. For the connectors to work with Oracle Identity Manager 11.1.2.2.0, you must complete the steps described in the section "Configuring Oracle Identity Manager 11.1.2 or Later" in the respective *Connector Guide*.
- Verify if the customizations made to the connectors are intact.
- Verify if the 11.1.2.2.0 related artifacts like UI Forms and Application Instances are generated.
- Ensure that all the operations of the connectors are working fine.
- If there are two or more IT Resource field in the process form, complete the steps described in the following My Oracle Support note:

  My Oracle Support document ID 1535369.1
- If there are any lookup query fields in the process form of the related connector, then you must customize the UI need to display the same. For more information, see 'Lookup Query' section in "General Customization Concepts" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

11.4.26 Updating the Provider URL For ForeignJNDIProvider-SOA

If the environment is running in SSL mode, you must change the **Provider URL** for **ForeignJNDIProvider-SOA** to SSL Provider URL. To do this, complete the following steps:

1. Log in to the WebLogic Administration console using the following URL:

   `http://weblogic_host:weblogic_port/console`
2. Expand **Services** under **Domain Structure**.
3. Click **Foreign JNDI Providers**.
4. Click **ForeignJNDIProvider-SOA** to bring up the **Settings for ForeignJNDIProvider-SOA** page.
5. Click **Lock & Edit** on the top-left pane.
6. In **Provider URL**, change **t3** to **t3s**.
7. Click **Save**, and then click **Activate Changes**.

11.4.27 Verifying the Upgrade

To verify your Oracle Identity Manager upgrade, perform the following steps:

1. Use the following URL in a web browser to verify that Oracle Identity Manager 11.1.2.2.0 is running:

   `http://<oim.example.com>:<oim_port>/sysadmin`

   `http://oim.example.com:14000/identity`

   where

<oim.example.com> is the path of the administration console.

<oim_port> is the port number.

2. Use Fusion Middleware Control to verify that Oracle Identity Manager and any other Oracle Identity Management components are running in the Oracle Fusion Middleware environment.
3. Install the Diagnostic Dashboard and run the following tests:
   - Oracle Database Connectivity Check
   - Account Lock Status
   - Data Encryption Key Verification
   - JMS Messaging Verification
   - SOA-Oracle Identity Manager Configuration Check
   - SPML Web Service
   - Test OWSM setup
   - Test SPML to Oracle Identity Manager request invocation
   - SPML attributes to Oracle Identity Manager attributes
   - Username Test

11.5 Troubleshooting

Note: For information about the issues that you might encounter during the upgrade process, and their workarounds, see *Oracle Fusion Middleware Release Notes*.

Table 11–19 lists some of the problems that might occur during the upgrade process, and their solutions:

Table 11–19 Oracle Identity Manager Troubleshooting - Problems and Solutions

Problem	Solution
Patch Set Assistant fails.	Check logs located at: On UNIX: <MW_HOME>/oracle_common/upgrade/logs/psa<time_stamp>.log On Windows: <MW_HOME>\oracle_common\upgrade\logs\psa<time_stamp>.log Fix the problem, and run Patch Set Assistant again.

Table 11–19 (Cont.) Oracle Identity Manager Troubleshooting - Problems and Solutions

Problem	Solution
Middle Tier upgrade fails	Check logs located at: On UNIX: ■ <OIM_ORACLE_HOME>/server/upgrade/logs/MT/OIMUpgrade<time_stamp>.log ■ <OIM_ORACLE_HOME>/server/upgrade/logs/MT/ant_JRF.log ■ <OIM_ORACLE_HOME>/server/upgrade./logs/MT/ant_PatchClasspath.log On Windows: ■ <OIM_ORACLE_HOME>\server\upgrade\logs\MT\OIMUpgrade<time_stamp>.log ■ <OIM_ORACLE_HOME>\server\upgrade\logs\MT\ant_JRF.log ■ <OIM_ORACLE_HOME>\server\upgrade.\logs\MT\ant_PatchClasspath.log
All features not upgraded in Middle Tier upgrade.	Check the Upgrade Report located at: On UNIX: <OIM_ORACLE_HOME>/upgrade/logs/MT/oimUpgradeReportDir/index.html On Windows: <OIM_ORACLE_HOME>\upgrade\logs\MT\oimUpgradeReportDir\index.html
Oracle Identity Manager upgrade control points.	Set the property value to `true` or `false` in the property file located at: On UNIX: <OIM_ORACLE_HOME>/server/bin/oimupgrade.properties On Windows: <OIM_ORACLE_HOME>\server\bin\oimupgrade.properties For more information, see Section 11.5.1, "Oracle Identity Manager Upgrade Control Points".
MDS patching issues.	Check the MDS Patching Report located at: On UNIX: <OIM_ORACLE_HOME>/server/logs/MDS_REPORT_DIRECTORY/MDSReport.html On Windows: <OIM_ORACLE_HOME>\server\logs\MDS_REPORT_DIRECTORY\MDSReport.html

Table 11–19 (Cont.) Oracle Identity Manager Troubleshooting - Problems and Solutions

Problem	Solution
Some MDS documents not merged correctly.	Merge manually from the following locations: On UNIX: ■ <OIM_ORACLE_HOME>/server/logs/sourceDir (OOTB MDS data location) ■ <OIM_ORACLE_HOME>/server/logs/targetDir (Your MDS data location) On Windows: ■ <OIM_ORACLE_HOME>\server\logs\sourceDir (OOTB MDS data location) ■ <OIM_ORACLE_HOME>\server\logs\targetDir (Your MDS data location)
JDBC errors: ORA-01882: timezone region not found	Add an additional environment variable, TZ, which is the time zone name, like GMT for example. The environment variable has to be set with older database or else you get an error. For more information, see My Oracle Support document ID 1460281.1.

11.5.1 Oracle Identity Manager Upgrade Control Points

Oracle Identity Manager Upgrade has provided some control points in the oimupgrade.properties. On UNIX, it is located in the <OIM_ORACLE_HOME>/server/bin/directory, on Windows, it is located in the <OIM_ORACLE_HOME>\server\bin\ directory.

You can selectively disable the feature upgrade by setting the property as false.

If any feature fails, you can continue with the upgrade by disabling the failed feature by setting the corresponding feature upgrade property as false.

As and when the solution is available for the failed feature, enable the feature for upgrade by setting the property to true.

By default, all the properties are set as true.

- Set the following property to false if you do not want to run Oracle Identity Manager configuration upgrade:

  oim.ps1.config.patch=true

- Set the following property to false if you do not want to run SOA composite upgrade:

  oim.ps1.soacomposite.patch=true

Domain Extension Properties

- Set the following property to false if you do not want to run Patch JNDI provider:

  oim.domainextension.jndiprovider.patch=true

- Set the following property to false if you do not want to run Patch ClassPath:

  oim.domainextension.classpath.patch=true

- Set the following property to false if you do not want to run Patch OPSS:

  oim.domainextension.opss.patch=true

- Set the following property to false if you do not want to run Patch ears:

```
oim.domainextension.ear.patch=true
```

- Set the following property to `false` if you do not want to run Patch JRF:

```
oim.domainextension.jrf.patch=true
```

12

Upgrading Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) Environment

This chapter describes how to upgrade your existing Oracle Entitlements Server 11*g* Release 1 (11.1.1.5.0) environment to Oracle Entitlements Server 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

This chapter includes the following sections:

- Section 12.1, "Upgrading Oracle Entitlements Server Administration Server"
- Section 12.2, "Upgrading Oracle Entitlements Server Client Server"

12.1 Upgrading Oracle Entitlements Server Administration Server

This section contains the following topics:

- Section 12.1.1, "Upgrade Roadmap for Oracle Entitlements Server Administration Server"
- Section 12.1.2, "Reviewing System Requirements and Certification"
- Section 12.1.3, "Shutting Down Administration Server and Managed Servers"
- Section 12.1.4, "Backing Up Oracle Entitlements Server 11g Release 1 (11.1.1.5.0)"
- Section 12.1.5, "Optional: Upgrading Oracle WebLogic Server"
- Section 12.1.6, "Upgrading Oracle Entitlements Server Administration Server 11g Release 2 (11.1.2.2.0)"
- Section 12.1.7, "Creating Oracle Platform Security Service Schema"
- Section 12.1.8, "Upgrading Oracle Platform Security Services Schema"
- Section 12.1.9, "Executing R2_Upgrade.sql"
- Section 12.1.10, "Creating New Oracle Entitlements Server Domain"
- Section 12.1.11, "Exporting Encryption Key"
- Section 12.1.12, "Re-Associating Policy Stores"
- Section 12.1.13, "Upgrading Oracle Platform Security Services"
- Section 12.1.14, "Starting the Administration Server and Oracle Entitlements Server Managed Servers"
- Section 12.1.15, "Redeploying APM"
- Section 12.1.16, "Verifying the Upgrade"

12.1.1 Upgrade Roadmap for Oracle Entitlements Server Administration Server

Note: If you do not follow the exact sequence provided in this task table, your Oracle Entitlements Server Administration Server upgrade may not be successful.

Table 12–1 lists the steps to upgrade Oracle Entitlements Server Administration Server upgrade.

Table 12–1 Upgrade Flow

Task No.	Task	For More Information
1	Review system requirements and certifications.	See, Reviewing System Requirements and Certification
2	Shut down all servers. This includes both Administration Server and Managed Servers.	See, Shutting Down Administration Server and Managed Servers
3	Back up your environment.	See, Backing Up Oracle Entitlements Server 11g Release 1 (11.1.1.5.0)
4	Optional - Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6.	See, Optional: Upgrading Oracle WebLogic Server
5	Upgrade 11.1.1.5.0 Oracle Home to 11.1.2.2.0.	See, Upgrading Oracle Entitlements Server Administration Server 11g Release 2 (11.1.2.2.0)
6	Create new Oracle Platform Security Services schema.	See, Creating Oracle Platform Security Service Schema
7	Upgrade Oracle Platform Security Services schema.	See, Upgrading Oracle Platform Security Services Schema
8	Execute R2_Upgrade.sql	See, Executing R2_Upgrade.sql
9	Create new Oracle Entitlements Server domain.	See, Creating New Oracle Entitlements Server Domain
10	Using the `exportEncryptionKey()`, extract the encryption key.	See, Exporting Encryption Key
11	Run the `configuresecuritystore.py` script to re-associate policy stores.	See, Re-Associating Policy Stores
12	Upgrade Oracle Platform Security Services.	See, Upgrading Oracle Platform Security Services
13	Start the Administration Server and Oracle Entitlements Server Managed servers.	See, Starting the Administration Server and Oracle Entitlements Server Managed Servers
14	Redeploy APM.	See, Redeploying APM
15	Verify the Oracle Entitlements Server upgrade.	See, Verifying the Upgrade

12.1.2 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements

for the products you are installing or upgrading. For more information see Section 2.1, "Reviewing System Requirements and Certification".

12.1.3 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Administration Server and Managed Servers.

For information about stopping the servers, see "Stopping the Servers" on page 2-10.

12.1.4 Backing Up Oracle Entitlements Server 11g Release 1 (11.1.1.5.0)

You must back up your Oracle Entitlements Server 11.1.1.5.0 environment before you upgrade to Oracle Entitlements Server 11.1.2.2.0.

After stopping the servers, back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Entitlements Server schemas

12.1.5 Optional: Upgrading Oracle WebLogic Server

Note:

- Upgrading Oracle WebLogic Server is not mandatory. However, Oracle recommends that you upgrade Oracle WebLogic Server to 10.3.6.
- If you upgrade Oracle WebLogic Server from 10.3.5 to 10.3.6, `weblogic.policy` will be overwritten. Hence, you must backup/restore some of the policies in `weblogic.policy`.

  After the upgrade procedure, add the following WebLogic Server SM policy:

```
grant codeBase "file:${oes.client.home}/-" {
permission java.security.AllPermission;
};
```

  In addition, if you had added any policies in 11.1.1.x.x, these policies must be backed up and restored after upgrading to 11.1.2.2.0.

You can upgrade WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6 by using the WebLogic 10.3.6 Upgrade Installer. For information about upgrading Oracle WebLogic Server, see "Upgrading to Oracle WebLogic Server 10.3.6" on page 2-2.

12.1.6 Upgrading Oracle Entitlements Server Administration Server 11*g* Release 2 (11.1.2.2.0)

To upgrade Oracle Entitlements Server Administration Server, you must use the Oracle Identity and Access Management 11.1.2.2.0 Installer. During the procedure, point the Middleware Home to your existing 11.1.1.5.0 Middleware Home. Your Oracle Home is upgraded from 11.1.1.5.0 to 11.1.2.2.0.

For information about upgrading Oracle Entitlements Server Administration Server 11g Release 1 (11.1.1.5.0), see "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)" on page 2-2.

12.1.7 Creating Oracle Platform Security Service Schema

Note: You must preform the following task only if your policy store is database.

Oracle Entitlements Server 11.1.1.5.0 schema is bound with APM. From Oracle Entitlements Server 11.1.2 release onwards, Oracle Entitlements Server security store relies on Oracle Platform Security Services for database. In order to access the Oracle Platform Security Services database, you need to create OPSS schema.

To create Oracle Platform Security Store (OPSS) schema, run the Repository Creation utility (RCU) 11.1.2.2.0. For more information, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

Note: In the **Select Components** screen, expand **AS Common Schemas** and select **Oracle Platform Security Services**. **Metadata Services** is selected automatically. Deselect it and ignore the following message:

```
Following components require Metadata Services schema:
Oracle Platform Security Services.
```

12.1.8 Upgrading Oracle Platform Security Services Schema

After updating the Oracle Entitlements Server binaries, you must upgrade the Oracle Platform Security Services schemas using Patch Set Assistant. To do this, complete the following steps:

1. Start the Patch Set Assistant from the location *MW_HOME*`/oracle_common/bin` using the following command:

   ```
   ./psa
   ```

2. Select **opss**.

3. Specify the Database connection details, and select the schema to be upgraded.

After you upgrade Oracle Platform Security Services schema, verify the upgrade by checking the log file at the location *MW_HOME*`/oracle_common/upgrade/logs/psa<`*timestamp*`>.log`.

The *timestamp* refers to the actual date and time when Patch Set Assistant was run. If the upgrade fails, check the log files to rectify the errors and run the Patch Set Assistant again.

For more information about upgrading schemas using Patch Set Assistant, see Section 2.6, "Upgrading Schemas Using Patch Set Assistant."

12.1.9 Executing R2_Upgrade.sql

After upgrading OPSS Schema, complete the following steps to migrate data from old store to new store.

1. Log in to the database as `SYS`.
2. Go to the following path:

   On UNIX:

   `<IAM_HOME>/oes/upgrade/sql`

   ON Windows:

   `<IAM_HOME>\oes\upgrade\sql`

3. Run the following sql script. Note that when you run this script, you must provide the 11.1.2.2.0 opss schema and 11.1.1.x.x APM schema details.

   `R2_Upgrade.sql`

   This sql script copies the user data from Oracle Entitlements Server 11.1.1.5.0 to Oracle Platform Security Services.

   Note: In order to execute the `R2_Upgrade.sql` command, you need to install a database client or execute the script in another computer that has a database client installed on it.

12.1.10 Creating New Oracle Entitlements Server Domain

Oracle Entitlements Server 11.1.2.2.0 Administration applications requires a JRF domain. But Oracle Entitlements Server 11.1.1.5.0 does not support JRF. Therefore, in order to deploy Oracle Entitlements Server 11.1.2.2.0 applications, you must create a new Oracle Entitlements Server domain.

For more information, see "Configuring Oracle Entitlements Server in a New WebLogic Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

12.1.11 Exporting Encryption Key

Credential data are encrypted and stored in the database. The encryption key is domain specific. Since you are moving to Oracle Entitlements Server 11.1.2.2.0 domain from Oracle Entitlements Server 11.1.1.5.0 domain, you must export the key to a keyfile and then import the key to the Oracle Entitlements Server 11.1.2.2.0 domain.

You must run the `exportEncryptionKey()` command to extract the encryption key from Oracle Entitlements Server 11.1.1.5.0 domain's bootstrap wallet.

Run the following command:

On UNIX:

1. Move from your present working directory to the `<MW_HOME>/oracle_common/common/bin` directory by running the following command on the command line:

   `cd <MW_HOME>/oracle_common/common/bin`

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. At the WLST prompt, run the following command:

   ```
   exportEncryptionKey(jpsConfigFile="<domaindir>/config/fmwconfig/jps-con
   fig.xml",keyFilePath="/tmp/key",keyFilePassword="<password>")
   ```

   where

   <domaindir> is the complete path of the Oracle Entitlements Server 11.1.1.5.0 domain location.

   <password> is the key file password.

On Windows:

1. Move from your present working directory to the <MW_HOME>\oracle_common\common\bin directory by running the following command on the command line:

   ```
   cd <MW_HOME>\orcle_common\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. At the WLST prompt, run the following command:

   ```
   exportEncryptionKey(jpsConfigFile="<domaindir>\\config\\fmwconfig\\jps-
   config.xml",keyFilePath="\\tmp\\key",keyFilePassword="<password>")
   ```

   Where

   <domaindir> is the complete path of the Oracle Entitlements Server 11.1.1.5.0 domain location.

   <password> is the key file password.

12.1.12 Re-Associating Policy Stores

You must re-associate policy stores to make the Oracle Entitlements Server 11.1.2.2.0 domain uptake the security store which is based on the Oracle Platform Security Services schema. Run the configuresecuritystore.py script to re-associate policy stores as follows:

12.1.12.1 Policy Store is DB

If the policy store in 11.1.1.5.0 is DB, perform the following steps to re-associate to DB based policy store and import the encryption key to the R2PS2 domain.

On UNIX:

Run the following WLST command:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <domaindir> -m join -j
<dwps1 jpsroot> -f <dwps1 farmname> -p <OPSS schema password> -t <policy
store type> -k <keyFilePath> -w <keyFilePassword> --create_diagnostic_data
```

For example:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <MW_HOME>/user_
```

```
projects/domains/<oes_domain> -m join -j cn=jpsroot -f <oes_domain> -p
welcome1 -t DB_ORACLE -k /tmp/key -w myKeyPwd --create_diagnostic_data
```

On Windows:

Run the following WLST command:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <domaindir> -m join -j
<OES 11.1.1.5.0 jpsroot> -f <OES 11.1.1.5.0 farmname> -p <OPSS schema
password> -t <policy store type> -k <keyFilePath> -w <keyFilePassword>
--create_diagnostic_data
```

For example:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <MW_HOME>\user_
projects\domains\<oes_domain> -m join -j cn=jpsroot -f oes_domain -p
welcome1 -t DB_ORACLE -k \tmp\key -w myKeyPwd --create_diagnostic_data
```

Note: For help on the command, run the following:

On UNIX:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <domaindir>
-help
```

On Windows:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <domaindir>
-help
```

Table 12–2 describes the parameters you need to specify on the command line.

Table 12–2 Parameters for Reassociating Policy Stores

Parameter	Description
`MW_HOME`	Specify the path to the Oracle Identity and Access Manager's Middleware Home. The following example shows the complete path: On UNIX, it is located in the `/oracle/Middleware` directory. On Windows, it is located in the `\oracle\Middleware` directory.
`IAM_HOME`	Specify the path to the Oracle Identity and Access Manager Home. The following example shows the complete path: On UNIX, it is located in the `/oracle/Middleware/Oracle_IDM1` directory. On Windows, it is located in the `\oracle\Middleware\Oracle_IDM1` directory.
`domaindir`	Specify the path to the Identity and Access Manager's domain location. The following example shows the complete path: On UNIX, it is located in the `<MW_HOME>/user_projects/domains/base_domain` directory. On Windows, it is located in the `<MW_HOME>\user_projects\domains\base_domain` directory.

Table 12–2 (Cont.) Parameters for Reassociating Policy Stores

Parameter	Description
-m	The following are the two options available for the argument -m: ■ create -m create option creates a new security store. This option is applicable for fresh installation. ■ join -m join option uses an existing database security store for the domain. Since this is an upgrade, you must use -m join option while running the configureSecurityStore.py command.
OPSS_schema_ password	Specify the password of OPSS schema.
-t	Specify the policy store type. For example: DB_ORACLE, DB_DERBY, or OID.
-k	Specify the path to the KeyFile. The following example shows the complete location: On UNIX, it is located at /tmp/key On Windows, it is located at \tmp\key
-w	Specify the KeyFile password.

12.1.12.2 Policy Store is OID

If the policy store in 11.1.1.5.0 is OID, perform the following steps to re-associate to OID based policy store and import the encryption key to the R2PS2 domain.

On UNIX:

Run the following WLST command:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <domaindir> -m join -j
cn=reassociate_r1ps1_oes_domain -f <dwps1 farmname> -t OID -a cn=orcladmin
-p <OPSS schema password> -l ldap://oim.example.com:18686 --create_
diagnostic_data
```

For example:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <MW_HOME>/user_
projects/domains/<oes_domain> -m join -j cn=jpsroot -f <oes_domain> -t OID
-a cn=orcladmin -p welcome1 -l ldap://oim.example.com:18686 --create_
diagnostic_data
```

On Windows:

Run the following WLST command:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <domaindir> -m join -j
cn=reassociate_r1ps1_oes_domain -f <OES 11.1.1.5.0 farmname> -t OID -a
cn=orcladmin -p <OPSS schema password> -l ldap://oim.example.com:18686
--create_diagnostic_data
```

For example:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <MW_HOME>\user_
```

```
projects\domains\<oes_domain> -m join -j cn=jpsroot -f oes_domain -t OID
-a cn=orcladmin -p welcome1 -l ldap://oim.example.com:18686 --create_
diagnostic_data
```

Note: For help on the command, run the following:

On UNIX:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <domaindir>
-help
```

On Windows:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <domaindir>
-help
```

Table 12–3 describes the parameters you need to specify on the command line.

Table 12–3 Parameters for Reassociating Policy Stores

Parameter	Description
`MW_HOME`	Specify the path to the Oracle Identity and Access Manager's Middleware Home. The following example shows the complete path: On UNIX, it is located in the `/oracle/Middleware` directory. On Windows, it is located in the `\oracle\Middleware` directory.
`IAM_HOME`	Specify the path to the Oracle Identity and Access Manager Home. The following example shows the complete path: On UNIX, it is located in the `/oracle/Middleware/Oracle_IDM1` directory. On Windows, it is located in the `\oracle\Middleware\Oracle_IDM1` directory.
`domaindir`	Specify the path to the Identity and Access Manager's domain location. The following example shows the complete path: On UNIX, it is located in the `<MW_HOME>/user_projects/domains/base_domain` directory. On Windows, it is located in the `<MW_HOME>\user_projects\domains\base_domain directory`.
`-m`	The following are the two options available for the argument `-m`: ■ `create` `-m create` option creates a new security store. This option is applicable for fresh installation. ■ `join` `-m join` option uses an existing database security store for the domain. Since this is an upgrade, you must use `-m join` option while running the `configureSecurityStore.py` command.
`OPSS_schema_password`	Specify the password of OPSS schema.

Table 12–3 (Cont.) Parameters for Reassociating Policy Stores

Parameter	Description
`-k`	Specify the path to the `KeyFile`. The following example shows the complete location: On UNIX, it is located at `/tmp/key` On Windows, it is located at `\tmp\key`
`-f`	Specify the security store farm name.
`-j`	Specify the distinguished name of `jpsroot`.
`-t`	Specify the policy store type. For example: `DB_ORACLE`, `DB_DERBY`, or `OID`.
`-a`	Specify the administrator username for OID.
`-l`	Specify the url for OID.

12.1.13 Upgrading Oracle Platform Security Services

After you upgrade schemas, you must upgrade Oracle Platform Security Services (OPSS) of the new Oracle Entitlements Server domain.

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Entitlements Server to 11.1.2.2.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see Section 2.7, "Upgrading Oracle Platform Security Services"

12.1.14 Starting the Administration Server and Oracle Entitlements Server Managed Servers

After the upgrade is complete, start the WebLogic Administration Server, the Administration Server for the domain that contains Oracle Entitlements Server, and the Oracle Entitlements Server Managed Server. For more information, see Section 2.9, "Starting the Servers".

12.1.15 Redeploying APM

To get the latest APM policies into the policy store, you must redeploy the APM applications.

Complete the following steps to redeploy APM:

On UNIX:

1. Move from your present working directory to the `<MW_HOME>/wlserver_10.3/common/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/wlserver_10.3/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following command:

```
redeploy(appName='oracle.security.apm')
```

5. Exit the WLST console using the `exit()` command.

On Windows:

1. Move from your present working directory to the `<MW_HOME>\wlserver_10.3\common\bin` by running the following command on the command line:

   ```
   cd <MW_HOME>\wlserver_10.3\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following command:

   ```
   <domaindir>\serverConfig\redeploy(appName='oracle.security.apm')
   ```

   where

   `<domaindir>` is the complete path to the Oracle Entitlements Server 11.1.2.2.0 domain.

   For example:

   ```
   <MW_HOME>\user_projects\domains\<oes_domain>\serverConfig\
   redeploy(appName='oracle.security.apm')
   ```

5. Exit the WLST console using the `exit()` command.

12.1.16 Verifying the Upgrade

To verify the Oracle Entitlements Server upgrade, do the following:

- Log in to LDAP or database and verify the schema version in the PolicyStore. The version number should be 11.1.1.7.2.0.
- The application MAPI works with both old and new functionalities.

  Create a new policy to see if CRUD operations on the policy store artifacts, using their entity managers, are working.

  For more information, see "Creating Fine Grained Elements for a Simple Policy" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*.
- The Application Runtime Authorization continues working.

  To verify, create an authorization, as mentioned in "Using the PEP API" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*, and see if it works correctly.

12.2 Upgrading Oracle Entitlements Server Client Server

This section contains the following topics:

- Section 12.2.1, "Upgrade Roadmap for Oracle Entitlements Server Client Server"
- Section 12.2.2, "Stopping all Security Module Instances"
- Section 12.2.3, "Upgrading Oracle Entitlements Server Client 11g Release 2 (11.1.2.2.0)"

- Section 12.2.4, "Changing Username and Password for the New Schemas"
- Section 12.2.5, "Starting the Security Modules"
- Section 12.2.6, "Verifying the Upgrade"

12.2.1 Upgrade Roadmap for Oracle Entitlements Server Client Server

Note: If you do not follow the exact sequence provided in this task table, your Oracle Entitlements Server Client Server upgrade may not be successful.

Table 12–4 lists the steps for upgrading Oracle Entitlements Server Client Server upgrade.

Table 12–4 Upgrade Flow

Sl. No.	Task	For More Information
1	Shut down all security modules. This includes shutting down the Administration Server and Managed Servers too.	See, Stopping all Security Module Instances
2	Upgrade 11.1.1.5.0 Oracle Home to 11.1.2.2.0.	See, Upgrading Oracle Entitlements Server Client 11g Release 2 (11.1.2.2.0)
3	Change the username and password.	See, Changing Username and Password for the New Schemas
4	Start the security modules.	See, Starting the Security Modules
5	Verify the Oracle Entitlements Server Client Server upgrade.	See, Verifying the Upgrade

12.2.2 Stopping all Security Module Instances

Bring down all security module instances, Administration Server, and Managed Servers.

The security module instances shuts down when the Administration Server and Managed Servers are shut down.

To stop the servers, see Section 12.1.3, "Shutting Down Administration Server and Managed Servers".

12.2.3 Upgrading Oracle Entitlements Server Client 11*g* Release 2 (11.1.2.2.0)

To upgrade Oracle Entitlements Server Client Server, you must use the 11.1.2.2.0 installer. During the procedure, point the Middleware Home to your existing 11.1.1.5.0 Oracle Entitlements Server Middleware Home. This upgrades your Middleware Home and Oracle Home from 11.1.1.5.0 to 11.1.2.2.0.

This section contains the following topics:

- Prerequisites
- Obtaining the Software
- Installing Oracle Entitlements Server Client Server 11g Release 2 (11.1.2.2.0)
- Verifying the Installation

12.2.3.1 Prerequisites

You must install and configure Oracle Entitlements Server Administration Server, as described in Section 12.1.6, "Upgrading Oracle Entitlements Server Administration Server 11g Release 2 (11.1.2.2.0)".

12.2.3.2 Obtaining the Software

For more information on obtaining Oracle Fusion Middleware 11*g* software, see *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.

12.2.3.3 Installing Oracle Entitlements Server Client Server 11*g* Release 2 (11.1.2.2.0)

For more information on installing Oracle Entitlements Server Client Server 11.1.2.2.0, see "Installing Oracle Entitlements Server Client" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

12.2.3.4 Verifying the Installation

To verify that your Oracle Entitlements Server Client install was successful, go to your Oracle Home directory which you specified during installation and verify that the Oracle Entitlements Server Client installation files are created.

12.2.4 Changing Username and Password for the New Schemas

If Oracle Entitlements Server client is running in a controlled-pull mode or in an uncontrolled mode, the `jps-config.xml` of the Security Module instance must be changed to reflect the schema changes done during the Administration Server upgrade.

Before running the `oessmconfig.sh` command, you need to modify `jps-config.xml` of the controlled-pull or uncontrolled security module.

Note: For Java, RMI and Web Service security modules, `jps-config.xml` is located at:

`<OES_CLIENT_HOME>/oes_sm_instances/<SM_NAME>/config`

For Oracle WebLogic Server security module, `jps-config.xml` is located at:

`<WLS_DOMAIN_HOME>/config/oeswlssmconfig/<SERVER_NAME>`

Note: For controlled-push security module, you do not have to add any parameters to the `pdp.service` instance.

Controlled-Pull Security Module

For controlled-pull security module, add the following to the `pdp.service` instance:

```
<property name="oracle.security.jps.runtime.pd.client.SMinstanceType"
value="<sm_type>"/>
```

Replace `"<sm_type>"` with the actual type.

For example:

```
"java"
```

Uncontrolled Security Module

For uncontrolled security module, add the following to the `pdp.service` instance:

```
<property
name="oracle.security.jps.runtime.pd.client.policyDistributionMode"
value="non-controlled"/>

<property name="oracle.security.jps.runtime.pd.client.sm_name" value="<sm_
name>"/>

<property name="oracle.security.jps.runtime.pd.client.SMinstanceType"
value="<sm_type>"/>
```

Replace `"<sm_name>" "<sm_type>"` with the actual values.

Do the following to change the username and password of the new schemas:

1. Go to the following path:

   On UNIX, `<CLIENT_HOME>/oesclient/oessm/enroll/bin`

   On Windows, `<CLIENT_HOME>\oesclient\oessm\enroll\bin`

2. Run the following command:

   On UNIX:

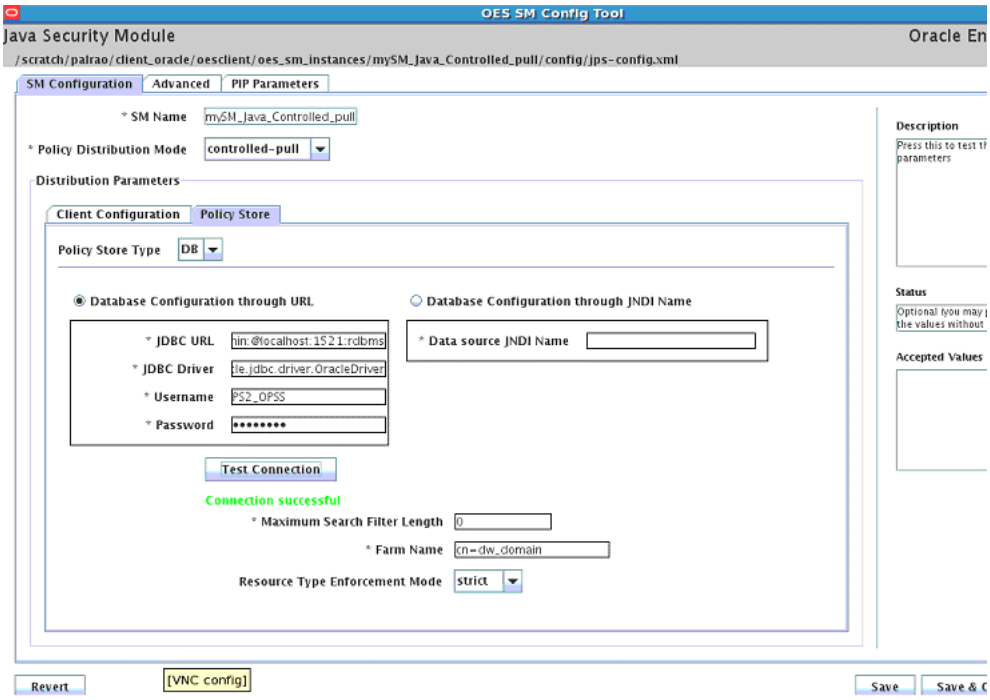
   ```
   ./oessmconfig.sh -jpsconfig <path to the jps-config.xml>
   ```

   On Windows:

   ```
   oessmconfig.cmd -jpsconfig <path to the jps-config.xml>
   ```

3. A Graphic User Interface displays. See Figure 12–1.
4. Click **SM Configuration**.
5. Click the **Policy Store** sub-tab.
6. Enter the new schema user name and password.
7. Click **Test Connection**
8. When you get the successful security module test message, click **Save & Close**.

Figure 12–1 Java Security Module



12.2.5 Starting the Security Modules

You must start the security modules by starting the Administration Server and Managed Servers.

To start the servers, see Section 12.1.14, "Starting the Administration Server and Oracle Entitlements Server Managed Servers".

12.2.6 Verifying the Upgrade

To verify, create an authorization, as mentioned in "Using the PEP API" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*, and see if it works correctly.

The Application Runtime Authorization continues working.

13

Upgrading Oracle Identity Navigator 11*g* Release 1 (11.1.1.x.x) Environments

This chapter describes how to upgrade your existing Oracle Identity Navigator 11*g* Release 1 (11.1.1.5.0) and 11*g* Release 1 (11.1.1.7.0) environments to Oracle Identity Navigator 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

> **Note:** This chapter refers to Oracle Identity Navigator 11g Release 1 (11.1.1.5.0) and 11g Release 1 (11.1.1.7.0) environments as 11.1.1.x.x.

This chapter includes the following sections:

- Upgrade Roadmap for Oracle Identity Navigator
- Reviewing System Requirements and Certification
- Exporting Oracle Identity Navigator 11.1.1.x.x Metadata
- Shutting Down Administration Server and Managed Servers
- Optional: Upgrading Oracle WebLogic Server
- Upgrading Oracle Identity Navigator 11g Release 2 (11.1.2.2.0)
- Creating Oracle Platform Security Services Schema
- Extending Oracle Identity Navigator 11.1.1.x.x Component Domains with Oracle Platform Security Services Template
- Upgrading Oracle Platform Security Services
- Configuring Oracle Platform Security Services Security Store
- Starting the Administration Server
- Verifying the Deployment Summary
- Upgrading Oracle Identity Navigator Application
- Importing the Oracle Identity Navigator 11.1.2.2.0 Metadata
- Verifying the Upgrade
- Optional: Configuring Oracle Identity Navigator on OPAM Managed Server

13.1 Upgrade Roadmap for Oracle Identity Navigator

Note: If you do not follow the exact sequence provided in this task table, your Oracle Identity Navigator upgrade may not be successful.

Table 13–1 lists the steps to upgrade Oracle Identity Navigator.

Table 13–1 Upgrade Flow

So. No.	Task	For More Information
1	Review system requirements and certifications.	See, Reviewing System Requirements and Certification
2	Export Oracle Identity Navigator data.	See, Exporting Oracle Identity Navigator 11.1.1.x.x Metadata
3	Shut down all servers. This includes both Administration Server and Managed Servers.	See, Shutting Down Administration Server and Managed Servers
4	Optional - Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6.	See, Optional: Upgrading Oracle WebLogic Server
5	Upgrade 11.1.1.x.x Oracle Home to 11.1.2.2.0.	See, Upgrading Oracle Identity Navigator 11g Release 2 (11.1.2.2.0)
6	Run Oracle Fusion Middleware Repository Creation Utility (RCU) to create and load OPSS schema for Oracle Identity and Access Management products.	See, Creating Oracle Platform Security Services Schema
7	Extend your Oracle Identity Navigator 11.1.1.x.x domain with the OPSS template.	See, Extending Oracle Identity Navigator 11.1.1.x.x Component Domains with Oracle Platform Security Services Template
8	Upgrade Oracle Platform Security Services.	See, Upgrading Oracle Platform Security Services
9	Run the `configuresecuritystore.py` script to configure policy stores.	See, Configuring Oracle Platform Security Services Security Store
10	Start the Administration Server.	See, Starting the Administration Server
11	Verify the deployments summary.	See, Verifying the Deployment Summary
12	Upgrade Oracle Identity Navigator.	See, Upgrading Oracle Identity Navigator Application
13	Import data.	See, Importing the Oracle Identity Navigator 11.1.2.2.0 Metadata
14	Verify the Oracle Identity Navigator upgrade.	See, Verifying the Upgrade
15	Optional - Configure Oracle Identity Navigator on the Oracle Privileged Account Manager Managed Server	See, Optional: Configuring Oracle Identity Navigator on OPAM Managed Server

13.2 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements for the products you are installing or upgrading. For more information see Section 2.1, "Reviewing System Requirements and Certification".

13.3 Exporting Oracle Identity Navigator 11.1.1.x.x Metadata

OINAV uses MDS as its metadata store. During upgrade, when you update the application, the metadata gets overwritten. Therefore, you need to export it and keep it in a temporary location so that it can be used to import original metadata after upgrade.

On the computer where Oracle Identity Navigator 11.1.1.x.x is installed, export the Oracle Identity Navigator metadata to an export directory using WLST as follows:

On UNIX:

1. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST (online) command:

   ```
   exportMetadata(application='oinav',server='AdminServer',toLocation='exp
   ort_directory')
   ```

   where

   `export_directory` is the directory where you want to export Oracle Identity Navigator metadata to.

On Windows:

1. Move from your present working directory to the `<IAM_HOME>\common\bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST (online) command:

   ```
   exportMetadata(application='oinav',server='AdminServer',toLocation='exp
   ort_directory')
   ```

   where

   `export_directory` is the directory where you want to export Oracle Identity Navigator metadata to.

13.4 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. So, before you begin the upgrade process, you must shut down the Administration Server and Managed Servers.

For information about stopping the servers, see "Stopping the Servers" on page 2-10.

13.5 Optional: Upgrading Oracle WebLogic Server

Oracle Identity and Access Management 11.1.2.2.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Identity Manager environment is using Oracle WebLogic Server 10.3.5 or the previous versions, you must upgrade Oracle WebLogic Server to 10.3.6.

For information about upgrading Oracle WebLogic Server, see "Upgrading to Oracle WebLogic Server 10.3.6" on page 2-2.

13.6 Upgrading Oracle Identity Navigator 11*g* Release 2 (11.1.2.2.0)

To upgrade Oracle Identity Navigator, you must use the Oracle Identity and Access Management 11.1.2.2.0 Installer. During the procedure, point the Middleware Home to your existing 11.1.1.x.x Oracle Identity Navigator Middleware Home. Your Oracle Home is upgraded from 11.1.1.x.x to 11.1.2.2.0.

For information about upgrading Oracle Identity Manager 11g Release 1 (11.1.1.x.x), see "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)" on page 2-2.

13.7 Creating Oracle Platform Security Services Schema

You must create Oracle Platform Security Services (OPSS) schema because Oracle Identity Navigator upgrade process involves OPSS schema policy store changes. The keys, roles, permissions, and other artifacts used by the applications must migrate to the policy store.

Run Repository Creation utility (RCU) to create OPSS schema.

For more information, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

Note: In the **Select Components** screen, expand **AS Common Schemas** and select **Oracle Platform Security Services**. The **Metadata Services** schema is selected automatically.

13.8 Extending Oracle Identity Navigator 11.1.1.x.x Component Domains with Oracle Platform Security Services Template

Oracle Identity Navigator 11.1.2.2.0 uses the database to store policies. This requires extending the 11.1.1.x.x Oracle Identity Navigator domain to include the OPSS data source.

To do so, complete the following steps:

1. Run the following command to launch the Oracle Fusion Middleware configuration wizard:

On UNIX:

`./config.sh`

It is located in the `<MW_HOME>/Oracle_IDM1/common/bin` directory.

On Windows:

`config.cmd`

It is located in the `<MW_HOME>\Oracle_IDM1\common\bin` directory.

2. On the **Welcome** screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
3. On the **Select a WebLogic Domain Directory** screen, browse to the directory that contains the WebLogic domain in which you configured the components. Click **Next**. The **Select Extension Source** screen is displayed.
4. On the **Select Extension Source** screen, select the **Oracle Platform Security Service - 11.1.1.0 [Oracle_IDM1]** option. After selecting the domain configuration options, click **Next**.
5. The **Configure JDBC Data Sources** screen is displayed. Configure the opssDS data source, as required. After the test succeeds, the **Configure JDBC Component Schema** screen is displayed.
6. On the **Configure JDBC Component Schema** screen, select the **Oracle Platform Security Services** schema.

   You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**.

   The **Test JDBC Component Schema** screen is displayed. After the test succeeds, the **Select Optional Configuration** screen is displayed.
7. On the **Select Optional Configuration** screen, you can configure Managed Servers, Clusters, and Machines and Deployments and Services. Do not select anything as you have already configured in your Oracle Identity Navigator 11.1.1.x.x environment. Click **Next**.
8. On the **Configuration Summary** screen, review the domain configuration, and click **Extend** to start extending the domain.

Your existing Oracle Identity Navigator domain is extended to support Oracle Platform Security Services (OPSS).

13.9 Upgrading Oracle Platform Security Services

After you upgrade schemas, you must upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Identity Navigator to 11.1.2.2.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see Section 2.7, "Upgrading Oracle Platform Security Services"

13.10 Configuring Oracle Platform Security Services Security Store

You must configure the Database Security Store as it is the only security store type supported by Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0).

For more information on configuring Oracle Platform Security Services, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

13.11 Starting the Administration Server

After the upgrade is complete, start the WebLogic Administration Server, the Administration Server that contains the Oracle Identity Navigator console.

For information about starting the Administration Server, see "Starting the Servers" on page 2-12.

13.12 Verifying the Deployment Summary

To verify the deployment summary, do the following:

1. Log in to the WebLogic Administration console:

   ```
   http://<admin server host>:<admin server port>/console
   ```

2. Under Domain Structure, click **Deployments**. The Summary of Deployments page is displayed.
3. Check the summary details and verify that **oinav (11.1.1.3.0)** is present in the Name table.

13.13 Upgrading Oracle Identity Navigator Application

Note: The OINAV version number is 11.1.1.3.0 while the Oracle Identity Navigator version number is 11.1.2.2.0.

This is not an error. The discrepancy is caused by a difference between how OINAV and Identity Access Management releases are tracked internally.

Upgrading Oracle Identity Navigator redeploys Oracle Identity Navigator using `oinav.ear` for Oracle Identity Navigator 11.1.2.2.0 release. There are two ways of redeploying the `oinav.ear`:

- Upgrading `oinav` using the WebLogic Server Administration Console.
- Upgrading `oinav` using the WebLogic Scripting Tool (WLST).

Using WebLogic Server Administration Console

Complete the following steps to upgrade Oracle Identity Navigator through the WebLogic Administration console:

1. Log in to WebLogic Administration console:

   ```
   http://<admin server host>:<admin server port>/console
   ```

2. Under Domain Structure, click **Deployments**.
3. Select **oinav (11.1.1.3.0)** from the **Name** table.
4. Click **Update** and click **Finish** in the **Update Application Assistant** screen after verifying the source path.

Note: If WebLogic is running in production mode, click **Lock & Edit** before clicking **Update.**

Using WebLogic Scripting Tool (WLST)

Complete the following steps to upgrade Oracle Identity Navigator through the WLST console:

On UNIX

1. Move from your present working directory to the `<MW_HOME>/wlserver_10.3/common/bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>/wlserver_10.3/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   connect('weblogic-username','weblogic-password','weblogic-url')

4. At the WLST prompt, run the following command:

   ```
   redeploy('oinav#11.1.1.3.0')
   ```

5. Exit the WLST console using the `exit()` command.

On Windows

1. Move from your present working directory to the `<MW_HOME>\wlserver_10.3\common\bin` directory by running the following command on the command line:

   ```
   cd <MW_HOME>\wlserver_10.3\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   connect('weblogic-username','weblogic-password','weblogic-url')

4. At the WLST prompt, run the following command:

   ```
   redeploy('oinav#11.1.1.3.0')
   ```

5. Exit the WLST console using the `exit()` command.

13.14 Importing the Oracle Identity Navigator 11.1.2.2.0 Metadata

You must import the metadata which was exported earlier so that Oracle Identity Navigator gets back the metadata present before upgrade. Import Oracle Identity Navigator 11.1.2.2.0 metadata by running the following WLST command:

On UNIX:

1. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST (online) command:

   ```
   importMetadata(application='oinav',server='AdminServer',fromLocation='e
   xport_directory')
   ```

   where

   `export_directory` is the directory where you have exported the Oracle Identity Navigator metadata to.

On Windows:

1. Move from your present working directory to the `<IAM_HOME>\common\bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>\common\bin
   ```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

   ```
   wlst.cmd
   ```

3. Connect to the Administration Server using the following command:

   ```
   connect('weblogic-username','weblogic-password','weblogic-url')
   ```

4. At the WLST prompt, run the following WLST (online) command:

   ```
   importMetadata(application='oinav',server='AdminServer',fromLocation='e
   xport_directory')
   ```

   where

   `export_directory` is the directory where you have exported Oracle Identity Navigator metadata to.

> **Note:** Oracle Business Intelligence Publisher 10*g* report format is not supported in Oracle Identity Navigator 11.1.2.2.0 release. It is not mandatory, but if you want to remove the reports, see "Configuring Oracle Business Intelligence Publisher" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*.

13.15 Verifying the Upgrade

To verify the Oracle Identity Navigator upgrade, do the following:

1. Log in to the OINAV console:

   ```
   http://<admin server host>:<admin server port>/oinav
   ```

2. In the Dashboard page, check for the version number in the bottom right corner.

   The version number should be 11.1.2.2.0.

13.16 Optional: Configuring Oracle Identity Navigator on OPAM Managed Server

To configure Oracle Identity Navigator on the Oracle Privileged Account Manager Managed server, do the following:

1. Stop the servers.
2. Move from your present working directory to the `<IAM_HOME>/common/bin` directory by running the following command on the command line:

   ```
   cd <IAM_HOME>/common/bin
   ```

3. Run the following command to launch the Oracle Fusion Middleware configuration wizard:

   On UNIX:

   ```
   ./config.sh
   ```

   On Windows:

   ```
   config.cmd
   ```

4. Select the **Extend an existing WebLogic domain** option, and select the OPAM domain.
5. Select **Oracle Identity Navigator for Managed Server** from the products. Select **Keep existing content** whenever it detects a conflict in the wizard.
6. Complete the configuration. Oracle Identity Navigator will run on the Oracle Privileged Account Manager Managed Server after starting the servers.

14

Upgrading Oracle Identity Manager 9.1.x.x Environments

This chapter describes how to upgrade Oracle Identity Manager 9.1.x.x to Oracle Identity Manager 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

This chapter includes the following sections:

- Upgrade Roadmap for Oracle Identity Manager
- Pre-Upgrade Steps
- Installing New Oracle Home and Upgrading Database Schemas
- Configuring Other Oracle Identity Manager Installed Components
- Upgrading Oracle Identity Manager 9.1.x.x Middle Tier
- Post-Upgrade Steps

14.1 Upgrade Roadmap for Oracle Identity Manager

The procedure for upgrading Oracle Identity Manager 9.1.x.xx to 11.1.2.2.0 involves the following high-level steps

1. **Pre-Upgrade Steps**: This step involves the necessary pre-upgrade tasks like reviewing system requirements and certification, generating the pre-upgrade report, analyzing the report and performing the necessary pre-upgrade tasks described in the report, backing up the existing 9.1.x.x environment.
2. **Installing New Oracle Home and Upgrading Database Schemas**: This step involves tasks like installing Oracle WebLogic Server, installing Oracle SOA Suite, installing Oracle Identity Manager binaries, upgrading Oracle Platform Security Services, upgrading JRF, upgrading Oracle Identity Manager and Oracle Platform Security Services schemas, creating the Oracle Identity Manager 11.1.2.2.0 domain, configuring database security store.
3. **Configuring Other Oracle Identity Manager Installed Components**: This step involves configuring Oracle Identity Manager Server, .
4. **Upgrading the Oracle Identity Manager Middle Tier**: This step involves tasks like upgrading Oracle Identity Manager middle tier.
5. **Post-Upgrade Steps**: This step involves any post-upgrade tasks like configuring Oracle Identity Manager Design Console, Oracle Identity Manager Remote Manger, and any other mandatory post-upgrade manual steps. This also invloves steps to verify the upgrade.

Table 14–1 lists the tasks to be completed to upgrade Oracle Identity Manager 9.1.x.x to 11.1.2.2.0.

Table 14–1 Roadmap for Upgrading Oracle Identity Manager 9.1.x.x to 11.1.2.2.0

Sl No	Task	For More Information
	Pre-Upgrade Steps	
1	Review the changes in the features of Oracle Identity Manager 11.1.2.2.0.	See, Feature Comparison
2	Review system requirements and certifications.	See, Reviewing System Requirements and Certification
3	Back up the Database used by your existing Oracle Identity Manager.	See, Backing Up Database Used by Oracle Identity Manager 9.1.x.x
4	Generate the pre-upgrade report, analyze the information provided in the report, and perform the necessary tasks described in the report before you proceed with the upgrade process.	See, Generating and Analyzing the Pre-Upgrade Report
5	Upgrade the OSI data by running the OSI data upgrade utility. If you have already performed this task as part of Generating and Analyzing the Pre-Upgrade Report, skip this section.	See, Upgrading the OSI Data
6	Ensure that xlconfig.xml has the correct values for the parameters `DirectDb` and `MultiCastAddress`.	See, Validating xlconfig.xml File
7	In Oracle Identity Manager 9.1.x.x, if you do not have at least one reconciliation field of type `ITResource`, then you must create one for all account type profiles.	See, Creating Reconciliation Field of Type IT Resource
	Installing New Oracle Home and Upgrading Database Schemas	
8	Create the necessary schemas required for the upgrade, using Repository Creation Utility.	See, Creating the Necessary Schemas
9	Install Oracle WebLogic Server 10.3.6.	See, Installing Oracle WebLogic Server 10.3.6
10	Install Oracle SOA Suite 11.1.1.7.0 which is used by Oracle Identity Manager 11.1.2.2.0. After you install SOA 11.1.1.7.0, you must apply mandatory SOA patches required for Oracle Identity Manager 11.1.2.2.0.	See, Installing Oracle SOA Suite 11.1.1.7.0 and Applying Mandatory SOA Patches
11	Install Oracle Identity Manager 11.1.2.2.0 using the Oracle Identity and Access Management 11.1.2.2.0 installer.	See, Installing Oracle Identity Manager 11.1.2.2.0
12	Upgrade Oracle Identity Manager schema using Upgrade Assistant.	See, Upgrading Oracle Identity Manager Schema

Table 14–1 (Cont.) Roadmap for Upgrading Oracle Identity Manager 9.1.x.x to 11.1.2.2.0

Sl No	Task	For More Information
13	Upgrade Oracle Platform Security Services schema using Patch Set Assistant.	See, Upgrading Oracle Platform Security Services Schema
14	Create a domain for Oracle Identity Manager 11.1.2.2.0 using the configuration wizard.	See, Creating a Domain for Oracle Identity Manager 11.1.2.2.0
15	Configure the Database security store.	See, Configuring Database Security Store
16	Start the WebLogic Administration Server and the SOA Managed Server(s).	See, Starting Administration Server and SOA Managed Server(s)
	Configuring Other Oracle Identity Manager Installed Components	
17	Configure the Oracle Identity Manager Server 11.1.2.2.0.	See, Configuring Oracle Identity Manager Server 11.1.2.2.0
18	Restart the WebLogic Administration Server and the SOA Managed Server(s).	See, Restarting the Administration Server and SOA Managed Server
	Upgrading the Oracle Identity Manager Middle Tier	
19	Start the Oracle Identity Manager Managed Server(s).	See, Starting and Stopping Oracle Identity Manager Managed Server(s)
20	Upgrade the Oracle Identity Manager middle tier.	See, Upgrading the Oracle Identity Manager Middle Tier
21	Restart the WebLogic Administration Server, SOA Managed Server(s), and the Oracle Identity Manager Managed Server(s).	See, Restarting all the Servers
	Post-Upgrade Steps	
22	Configure the Oracle Identity Manager Design Console 11.1.2.2.0.	See, Optional: Configuring the Oracle Identity Manager Design Console 11.1.2.2.0
23	Configure the Oracle Identity Manager Remote Manager 11.1.2.2.0.	See, Optional: Configuring the Oracle Identity Manager Remote Manager 11.1.2.2.0
24	Perform all the necessary post-upgrade tasks.	See, Performing Post-Upgrade Tasks
25	Verify the Oracle Identity Manager 9.1.x.x upgrade.	See, Verifying the Upgrade

14.2 Pre-Upgrade Steps

This section describes all the pre-upgrade steps that you must complete before you start upgrading the Oracle Identity Manager 9.1.x.x environment. This section includes the following topics:

- Feature Comparison

- Reviewing System Requirements and Certification
- Backing Up Database Used by Oracle Identity Manager 9.1.x.x
- Generating and Analyzing the Pre-Upgrade Report
- Upgrading the OSI Data
- Validating xlconfig.xml File
- Creating Reconciliation Field of Type IT Resource

14.2.1 Feature Comparison

Table 14–2 lists key differences in functionality between Oracle Identity Manager 9.1.x.x and Oracle Identity Manager 11.1.2.2.0.

Table 14–2 Features Comparison

Oracle Identity Manager 9.1.x.x	Oracle Identity Manager 11.1.2.2.0
Oracle Identity Manager 9.1.x.x provides Identity Attestation to periodically review a user's access. For advanced access review capabilities such as role or data owner certification, OIM 9.1.x.x had to be integrated with Oracle Identity Analytics (OIA) to leverage the advanced access review capabilities that OIA provided.	In Oracle Identity Manager 11.1.2.2.0, the advanced access review capabilities of OIA are converged into OIM to provide a complete identity governance platform that enables an enterprise to do enterprise grade access request, provisioning, and access review from a single product. After upgrading to Oracle Identity Manager 11.1.2.2.0, you can use the new access review capabilities. This feature is disabled by default. You must ensure that you have relevant licenses before enabling this new feature.
In Oracle Identity Manager 9.1.x.x, users are assigned to organizations by specifying an organization name in the Organization attribute of the user details. This is a static organization membership. A user can only be a member of one organization.	In Oracle Identity Manager 11.1.2.2.0, in addition to the existing feature, you can dynamically assign users to organizations based on user-membership rules, which you can define in the `Members` tab of the organization details page. All users who satisfy the user-membership rule are dynamically associated with the organization, irrespective of the organization hierarchy the users statically belong to. With this new capability, a user can gain membership of one home organization via static membership and multiple secondary organizations via user-membership rules that are dynamically evaluated. Post upgrade, organization can uptake this new capability by defining membership rules for each organization.

Table 14–2 (Cont.) Features Comparison

Oracle Identity Manager 9.1.x.x	Oracle Identity Manager 11.1.2.2.0
Oracle Identity Manager 9.1.x.x provides basis self service capabilities such as password reset and account request.	Oracle Identity Manager 11.1.2.2.0 provides a new user interface with a shopping cart type request model through which end users can search and browse through the catalog and directly request any item like roles, entitlements, or applications without having to navigate through a series of menus. In addition to this, additional business friendly metadata such as description, audit objective, tags, owner, approver, and technical glossary can be associated to each access item to display business friendly and rich contextual information to a business user at the time of self service access request and access review. An end user access to request-able entities is controlled by a combination of user to organization publishing and entity to organization publishing. Post upgrade, administrators need to run the catalog synchronization job to populate the catalog with request-able entities and entity metadata. Post upgrade administrators need to define entity to organization publishing to control what an end user can request for.
Oracle Identity Manager 9.1.x.x Resource and IT resource names tend to be named in a manner such that it is easy for the IT users to manage them. The problem with this approach is that if a business user has to request access the resource name will not make sense to him/her. These incomprehensible Resource and IT resource names make the access request process non-intuitive.	Oracle Identity Manager 11.1.2.2.0 provides an abstraction entity called Application Instance. It is a combination of IT resource instance (target connectivity and connector configuration) and resource object (provisioning mechanism). Administrators can assign business friendly names to Application instances and map them to corresponding IT resources and Resource Objects. End user who request for accounts through the catalog will search for an account by providing the business friendly Application Instance Name. Application instances are automatically created as part of the Upgrade procedure. Administrators are expected to define organization publishing for these Application Instances to control who has access to request for access to the application. Any changes in the display names of request-able entities should be added to the end user training program.

Table 14–2 (Cont.) Features Comparison

Oracle Identity Manager 9.1.x.x	Oracle Identity Manager 11.1.2.2.0
Oracle Identity Manager 9.1.x.x security model gives an organization the ability to grant and manage delegated administration of entities, such as users, organizations, and roles. Delegation is managed via Administrative Groups and permission granted to those administrative groups.	Oracle Identity Manager 11.1.2.2.0 leverages Oracle Entitlement Server for authorization policy enforcement and administration. This is the standards based platform for authorization policy enforcement and administration across all IDM components. An end user's authorization to business functions is scoped based on admin roles that have been granted to him/her within the scope of an organization. Post upgrade to Oracle Identity Manager 11.1.2.2.0 an administrator will have to assign admin roles to an end user to enable delegated administration; they will have to assign these admin roles within the scope of an organization. Administration of Authorization Policies is done via the Authorization Policy Manager which is the de facto tool for lifecycle management of Authorization policies. Post upgrade, authorization policy definition and administration needs to be done from the Authorization Policy Manager.
In Oracle Identity Manager 9.1.x.x, access policy evaluation is done instantly for each user when they were updated.	In Oracle Identity Manager 11.1.2.2.0, access policy evaluation is done when the Evaluate User Policies scheduled job is run. This gives you the flexibility to control when heavy operations such as access policy evaluation and provisioning are triggered. Post upgrade to Oracle Identity Manager 11.1.2.2.0, you must schedule this job to run in predefined intervals based on their business requirements.
The Oracle Identity Manager 9.1.x.x User Interface is built on the struts framework. It provides basic self service interfaces.	Oracle Identity Manager 11.1.2.2.0 provides a rich and business friendly UI that is built on Oracle ADF and Web Composer technology Any customization added to the 9.1.x.x UI needs to be reapplied on the 11.1.2.2.0 UI post upgrade. Refer to the Customizing the Interface section in the Developers Guide for an overview of UI customization in Oracle Identity Manager 11.1.2.2.0.

Table 14–2 (Cont.) Features Comparison

Oracle Identity Manager 9.1.x.x	Oracle Identity Manager 11.1.2.2.0
Oracle Identity Manager 9.1.x.x access policies provides the option to revoke or do nothing to an account when a user loses membership of a role that provisioned the user's account via the access policy.	Oracle Identity Manager 11.1.2.2.0 access policies provides the option to revoke or disable an account when a user loses membership of a role that provisioned the user's account via the access policy. When you upgrade to Oracle Identity Manager 11.1.2.2.0, policies which had the `Revoke if no longer applies` option deselected will be converted to `Disable if no longer applies`. Users associated with these policies will not be updated, but any future updates to the policy will result in the user being marked with a `Disable if no longer applies` flag. Access policies have also been significantly enhanced to support improved automated provisioning of multiple accounts in the same instance of target application to the same user, as well as automated provisioning of multiple accounts in different instances of the same target application. This added capability reduces the need for cloning of objects and improve performance.
Oracle Identity Manager 9.1.x.x requires administrators to define approval processes from the design console and one approval process must be configured per managed Application or Resource object.	Oracle Identity Manager 11.1.2.2.0 uses SOA composite for Approval orchestration and notifications. The benefit with this model is that administrators can define a single approval workflow (SOA Composite) and use is for multiple Applications. SOA infrastructure also provides a robust monitoring, diagnostics and management platform that can be immediately leveraged post upgrade. Post upgrade, you must transform 9.1.x.x approval processes to SOA composites and configure notification within these composites.

Table 14–2 (Cont.) Features Comparison

Oracle Identity Manager 9.1.x.x	Oracle Identity Manager 11.1.2.2.0
In Oracle Identity Manager 9.1.x.x, Entity Adapters and Event handlers are used to customize operations on entities like User and Role. They are frequently used to populate attributes for entities like User and Role at various lifecycle events like pre-update, pre-delete, pre-insert, post-insert, post-update, or post-delete.	Oracle Identity Manager 11.1.2.2.0 uses the plug-in framework to support customizations to operations on entities. The Plug-in Framework allows customers to easily extend and customize the capabilities of the out-of-the-box Oracle Identity Manager features. The features expose specific plug-in points in the business logic where extensibility can be provided. An interface definition accompanies each such point and is called the plug-in interface. Customers can create code that extends these plug-in interfaces and defines customizations based on their business needs. These plug-ins are deployed and registered with Oracle Identity Manager by using the Plug-in Manager. Oracle Identity Manager then incorporates the plug-ins into the feature processing from that point onward. Post upgrade, the organization needs to transform 9.1.x.x event handlers, entity adapters, and pre populate adapters into plug-ins.

14.2.2 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see Section 2.1, "Reviewing System Requirements and Certification".

14.2.3 Backing Up Database Used by Oracle Identity Manager 9.1.x.x

You must back up your existing Oracle Identity Manager 9.1.x.x environment before you upgrade to Oracle Identity Manager 11.1.2.2.0.

After stopping the servers, back up the following:

- *MW_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Identity Manager schemas

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

14.2.4 Generating and Analyzing the Pre-Upgrade Report

You must run the `PreUpgradeReport` utility before you begin the upgrade process, and address all the issues listed as part of this report with the solution provided in the report. The `Pre-UpgradeReport` utility analyzes your existing Oracle Identity Manager 9.1.x.x environment, and provides information about the mandatory prerequisites that you must complete before you upgrade the existing Oracle Identity Manager environment.

The information in the pre-upgrade report is related to the pending audit tasks, cyclic dependencies in LDAP that need to be removed, tasks related to offline provisioning, status of the mandatory database components and settings, status of OSI data upgrade, potential application instance creation issues, pending reconciliation events, and pending requests.

Note: Run this report until no pending issues are listed in the report.

It is important to address all the issues listed in the pre-upgrade report, before you can proceed with the upgrade, as upgrade might fail if the issues are not fixed.

To generate and analyze the pre-upgrade report, complete the tasks described in the following sections:

- Obtaining Pre-Upgrade Report Utility
- Generating the Pre-Upgrade Report
- Analyzing the Pre-Upgrade Report

14.2.4.1 Obtaining Pre-Upgrade Report Utility

You must download the pre-upgrade utility from Oracle Technology Network (OTN). The utility is available in two zip files named `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002`, along with `ReadMe.doc` at the following location on My Oracle Support:

My Oracle Support document ID 1599043.1

The `ReadMe.doc` contains information about how to generate and analyze the pre-upgrade reports.

14.2.4.2 Generating the Pre-Upgrade Report

To generate the pre-upgrade report for Oracle Identity Manager 9.1.x.x upgrade, do the following:

1. Create a directory at any location and extract the contents of `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002` in the newly created directory.
2. Create a directory where pre-upgrade reports need to be generated. For example, name the directory *`OIM_preupgrade_reports`*.
3. Go to the directory where you extracted `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002`, and open the `preupgrade_report_input.properties` file in a text editor. Update the properties file by specifying the appropriate values for the parameters listed in Table 14–3:

Table 14–3 Parameters to be Specified in the preupgrade_report_input.properties File

Parameter	Description
`oim.targetVersion`	Specify `11.1.2.2.0` for this parameter, as `11.1.2.2.0` is the target version for which pre-upgrade utility needs to be run.
`oim.jdbcurl`	Specify the JDBC URL for Oracle Identity Manager in the following format: *`<host>:<port>/<service_name>`*

*Table 14–3 (Cont.) Parameters to be Specified in the preupgrade_report_*

Parameter	Description
oim.oimschemaowner	Specify the name of the OIM schema owner.
oim.databaseadminname	Specify the user with DBA privilege. For example, sys as sysdba.
oim.outputreportfolder	Specify the absolute path to the directory that you created in step-2 (directory with name *OIM_preupgrade_reports*), where the pre-upgrade reports need to be generated. Make sure that the output report folder has read and write permissions.
oim.domain	Specify the absolute path to the Oracle Identity Manager domain home. For example: /Middleware/user_projects/domains/base_domain

4. Set the environment variables JAVA_HOME by running the following command:

   On UNIX:

   ```
   export JAVA_HOME=<absolute_path_to_jdk_location>
   ```

   On Windows:

   ```
   set JAVA_HOME="<absolute_path_to_jdk_location>"
   ```

5. Run the following command from the location where you extracted the contents of PreUpgradeReport.zip.001 and PreUpgradeReport.zip.002:

   - **On UNIX**:

     ```
     sh generatePreUpgradeReport.sh
     ```

   - **On Windows**:

     ```
     generatePreUpgradeReport.bat
     ```

6. Provide the details when the following is prompted:

   - **OIM Schema Password**

     You must enter the password of the OIM schema.

   - **DBA Password**

     You must enter the password of the Database Administrator.

7. The pre-upgrade report utility generates the reports as HTML pages at the location you specified for the parameter oim.outputreportfolder in the preupgrade_report_input.properties file. The logs are stored in the log file preUpgradeReport<*time*>.log in the folder logs at the same location.

   The following are the reports generated by the pre-upgrade report utility:

   - index.html
   - AUDITPreUpgradeReport.html
   - CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html
   - JMSPreUpgradeReport.html
   - ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html

- OSIPreUpgradeReport.html
- PasswordPolicyPreUpgradeReport.html
- PROVISIONINGPreUpgradeReport.html
- RECONPreUpgradeReport.html
- REQUESTPreUpgradeReport.html

14.2.4.3 Analyzing the Pre-Upgrade Report

After you generate the pre-upgrade reports, you must review each of the reports, and perform all the tasks described in them. If you do not perform the mandatory tasks described in the report before you upgrade, the upgrade might fail.

Table 14–4 lists all the pre-upgrade reports, describes what information each report contains, and provides links to the detailed description of each report.

Table 14–4 Description of Pre-Upgrade Reports

HTML Report Name	Description	For Detailed Description
index.html	This report provides links to all the other reports generated by the pre-upgrade report utility. It also states that you must run the pre-upgrade report utility till no pending issues are listed in this report.	See, Description of index.html Report
AUDITPreUpgradeReport.html	This report lists the pending audit tasks that you need to perform before you start the upgrade process.	See, Description of AUDITPreUpgradeReport.html Report
CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html	This report detects and displays the list of cyclic groups in LDAP. Cyclic groups in LDAP directory are not supported in 11.1.2.2.0. Therefore, you must remove the cyclic dependency from Oracle Identity Manager 9.1.x.x setup and reconcile data from LDAP to Oracle Identity Manager Database. The procedure for doing this is described in the report.	See, Description of CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html Report
JMSPreUpgradeReport.html	This report lists the pending tasks related to offline provisioning.	See, Description of JMSPreUpgradeReport.html Report
ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html	This report provides the status of the mandatory database components or settings for Oracle Identity Manager upgrade. Verify the installation or setup status for each of the mandatory component or setting. If any of the component or setting is not setup correctly, follow the recommendations provided in the report to fix them.	See, Description of ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html Report

Table 14–4 (Cont.) Description of Pre-Upgrade Reports

HTML Report Name	Description	For Detailed Description
`OSIPreUpgradeReport.html`	This report gives the status of the OSI data upgrade. If the report states that the OSI data upgrade is not applied, then upgrade OSI data as described in Section 14.2.5, "Upgrading the OSI Data".	See, Description of OSIPreUpgradeReport.html Report
`PasswordPolicyPreUpgradeReport.html`	This report lists the potential upgrade issues for password policies. If you are relying on 9.1.x.x password policy model, you must update to new password policies, as 9.1.x.x password policy model is not supported in 11.1.2.2.0. Review the report and assign the password policies listed in the report to appropriate organization(s).	See, Description of PasswordPolicyPreUpgradeReport.html Report
`PROVISIONINGPreUpgradeReport.html`	This report lists the potential application instance creation issues. It provides information about the following: ■ Provisioning Configuration ■ Entitlement Configuration ■ Access Policy Configuration ■ List of Resource Objects without Process Form ■ List of Resource Objects without ITResource field Type in Process Form ■ List of Resource Objects with multiple ITResource Lookup fields in Process Form ■ List of Access Policies without ITResource value set in default policy data ■ List of Access Policies with Revoke If No Longer Applies flag unchecked ■ List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value Review all the sections in the report and perform necessary tasks.	See, Description of PROVISIONINGPreUpgradeReport.html Report
`RECONPreUpgradeReport.html`	This report lists all the pending reconciliation events. Review the information provided in the report.	See, Description of RECONPreUpgradeReport.html Report

Table 14–4 (Cont.) Description of Pre-Upgrade Reports

HTML Report Name	Description	For Detailed Description
REQUESTPreUpgradeReport.html	This report lists all the pending requests. Review the information provided in the report.	See, Description of REQUESTPreUpgradeReport.html Report
ORACLE_ONLINE_PURGE_PreUpgradeReport.html	This report lists the pre-requisites for Online Purge that needs to be addressed before you proceed with the upgrade. This report will not be generated if they is no action item related to purge.	See, Description of ORACLE_ONLINE_PURGE_PreUpgradeReport.html Report

14.2.4.3.1 Description of index.html Report This index.html is the index page that contains links to the other reports.

Table 14–5 lists the reports displayed in `index.html` and their corresponding HTML report names.

Table 14–5 Reports Listed in index.html and Their Corresponding HTML Report Names

Report Name in index.html	Corresponding HTML Report
Installation Status of Mandatory Database Components	ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html
Pending Audit Tasks	AUDITPreUpgradeReport.html
Pending Recon Events	RECONPreUpgradeReport.html
Pending Approval Tasks	REQUESTPreUpgradeReport.html
Pending Offline Provisioning Tasks	JMSPreUpgradeReport.html
OSI Data Upgrade Utility Status	OSIPreUpgradeReport.html
List of invalid Password Policies	PasswordPolicyPreUpgradeReport.html
List of cyclic groups in LDAP directory	CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html
List of potential app instance creation issues	PROVISIONINGPreUpgradeReport.html

14.2.4.3.2 Description of AUDITPreUpgradeReport.html Report The report `AUDITPreUpgradeReport.html` lists all the pending audit tasks.

14.2.4.3.3 Description of CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html Report The report `CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html` provides information about the Cyclic groups in LDAP directory.

Oracle Identity Manager 11.1.2.2.0 does not support cyclic groups in the LDAP directory. Therefore, you must remove the cyclic dependency from Oracle Identity Manager 9.1.x.x setup and reconcile data from LDAP to Oracle Identity Manager Database, before you proceed with the upgrade.

For more information about removing the cyclic groups dependent on LDAP, see Removing Cyclical Groups Dependent on LDAP and Reconciling Data From LDAP to OIM Database. The procedure for removing cyclic groups is also described in this report.

Removing Cyclical Groups Dependent on LDAP and Reconciling Data From LDAP to OIM Database

If the LDAP in your Oracle Identity Manager 9.1.x.x environment has cyclic groups loaded, you must remove the cyclic groups by doing the following:.

1. Use JEXplorer or Softerra LDAP Administrator and navigate to the cyclic groups.
2. Look for **uniquemember** attribute.
3. Remove all values from the attribute.
4. Save the group.
5. Reconcile the data from LDAP to Oracle Identity Manager Database by running the following command:

   On UNIX: `LDAPConfigPostSetup.sh`

   On Windows: `LDAPConfigPostSetup.bat`

Example Scenario

If you have cyclic group dependency between two groups: Group1 and Group2, do the following to remove cyclic dependency:

1. Connect to LDAP using JEXplorer or Softerra LDAP.
2. Go to the group container of Group1.
3. Go to the **uniquemember** attribute under Group1.
4. Remove the value of Group2, from unique members, and save the change made.
5. Run `LDAPConfigPostSetup.sh` (on UNIX) or `LDAPConfigPostSetup.bat` (on Windows) to reconcile data from LDAP to Oracle Identity Manager database.

14.2.4.3.4 Description of JMSPreUpgradeReport.html Report The report `JMSPreUpgradeReport.html` lists all the pending offline provisioning tasks. The report contains a table with the package name, task status key, offline flag, request key, and object key. You must review the information provided in this report.

14.2.4.3.5 Description of ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html Report The report `ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html` lists all the mandatory database components or settings for Oracle Identity Manager 9.1.x.x upgrade. This report contains a table which lists the component or setting, it's installation or setup status, and recommendations if any. You must review the installation or setup status for each of the mandatory component or setting listed in the table. If the component or setting is not setup correctly, follow the recommendations specified in the **Note** column of the table in the report to fix them.

14.2.4.3.6 Description of OSIPreUpgradeReport.html Report The report `OSIPreUpgradeReport.html` provides the status of the OSI data upgrade. If the report states that the OSI data upgrade utility is not applied yet, you must run the OSI data upgrade utility to upgrade OSI data as described in Section 14.2.5, "Upgrading the OSI Data".

If the reports states that the OSI data upgrade utility is already applied, no action is required.

14.2.4.3.7 Description of PasswordPolicyPreUpgradeReport.html Report The report `PasswordPolicyPreUpgradeReport.html` lists the potential upgrade issues for password policies. If you are using 9.1.x.x password policy model, you must update them to new password policies. The 9.1.x.x password policy model is no longer supported for `Users`, and any such customizations done are not migrated to the new password policy model. A default password policy is seeded at `TOP` organization that needs to be revisited.

This report contains a table that lists the password policies that are attached to the `Xellerate User` resource object according to the 9.1.x.x password policy model. You must assign those password policies to appropriate organization(s).

14.2.4.3.8 Description of PROVISIONINGPreUpgradeReport.html Report The report `PROVISIONINGPreUpgradeReport.html` lists the potential application instances creation issues. The report contains the following sections:

- Provisioning, Entitlement, and Access Policy Configuration Details
- List of Resource Objects without Process Form
- List of Resource Objects without ITResource field Type in Process Form
- List of Resource Objects with multiple ITResource Lookup fields in Process Form
- List of Access Policies without ITResource value set in default policy data
- List of Access Policies with Revoke If No Longer Applies flag unchecked
- List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value

Provisioning, Entitlement, and Access Policy Configuration Details

This section describes the steps you must complete before you upgrade Oracle Identity Manager 9.1.x.x to 11.1.2.2.0. These steps are related to provisioning, entitlement, and access policy configuration. Complete all the steps described in this section of the report.

List of Resource Objects without Process Form

This section provides information about the resource objects in Oracle Identity Manager 9.1.x.x that do not have process form. Each resource object must have a process form associated with it. Therefore, if a resource object is not associated with a process form, you must associate the resource object with a process form before you start the upgrade process. Review the table in this section of the report, that lists the details of the resource objects without process form.

List of Resource Objects without ITResource field Type in Process Form

This section provides information about the resource objects without ITResource field type in their respective process forms. Review the table in this section of the report, which contains more details. If your Oracle Identity Manager 9.1.x.x has resource objects without ITResource field in their process forms, do the following:

1. Create appropriate IT resource definition.
2. Create IT resource instance for the same corresponding to the target that is being provisioned.

3. Edit the process form and add a field of type "ITResource" to the process form. Set the following properties:

   Type=*IT Resource definition created in step-1*

   ITResource=true

4. Activate the form.
5. Update the IT resource field on existing provisioned accounts using FVC Utility.
6. Once the above steps are completed, you can create application instances corresponding to the Resource Object+ITResource combination.

List of Resource Objects with multiple ITResource Lookup fields in Process Form

This section provides information about the resource objects that have multiple lookup fields in their process form. In the Oracle Identity Manager 9.1.x.x environment, if you have resource objects with multiple ITResource set in the process form, you must set the value of the property ITResource Type to true for at least one of the attributes.

List of Access Policies without ITResource value set in default policy data

This section lists the access policies for which the ITResource values of the resource objects should be set in the default policy data. The table in this section lists the access policies in Oracle Identity Manager 9.1.x.x for which ITResource field is missing. You must set the values of ITResurce field for each of the access policy listed in the table.

List of Access Policies with Revoke If No Longer Applies flag unchecked

This section lists the access policies that have Revoke If No Longer Applies flag unchecked. The table in this section contains the list of access policies that will be updated to Disable If No Longer Applies, during upgrade. The table also indicates if tasks for enable, disable, revoke actions are not defined for these policies. You must add the missing tasks before you proceed with the upgrade. Also, if you want the behavior of the policy to change to RNLA checked, you must check the RNLA flag for the respective policy.

List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value

This section lists entitlements stored in lookup definitions that do not have IT Resource Key pretended to their encoding values using "~". Entitlements stored in lookup definitions need IT Resource Key prepended to the encoded values using "~". Review the table in this section of the pre-upgrade report, which contains more details.

14.2.4.3.9 Description of RECONPreUpgradeReport.html Report The report RECONPreUpgradeReport.html lists all the pending reconciliation events. The report contains a table that lists all the pending reconconciliation events with their recon ID, recon date, recon status, and recon-by data. You must review the information provided in the table.

14.2.4.3.10 Description of REQUESTPreUpgradeReport.html Report The report REQUESTPreUpgradeReport.html lists all the pending requests. The report contains a table that lists all the pending requests with their request ID, request date, request-by details, request status, and request data. You must review the information provided in the table.

14.2.4.3.11 Description of ORACLE_ONLINE_PURGE_PreUpgradeReport.html Report Before you upgrade Oracle Identity Manager 9.1.x.x to 11.1.2.2.0, you must complete the pre-requisites for online purge.

The table in this report lists the database tables on which the mentioned pre-upgrade steps need to be performed before you upgrade. The table also shows the status of the database tables in **OIM schema** and **Note** section. Review the table, and perform the actions required.

14.2.5 Upgrading the OSI Data

This section describes how to upgrade OSI data.

> **Note:** If you have already performed this task as part of Section 14.2.4, "Generating and Analyzing the Pre-Upgrade Report", skip this section.

The format of values stored in the internal column `osi_note` which contains transient values used in processes, is different in Oracle Identity Manager 11.1.2.2.0 when compared to Oracle Identity Manager 9.1.x.x. As the format of the values are incompatible, you must clean the existing values using the OSI Data Upgrade utility before you proceed with the upgrade. The OSI Data Upgrade utility upgrades the OSI data.

> **Note:** OIM 9.1.0.x server is not expected to be running after you upgrade the OSI data.
>
> Depending on the amount of data in OSI, the OSI data upgrade may take some time.

For information about obtaining the OSI Data Upgrade utility and running the utility to upgrade OSI data, see My Oracle Support Document ID 1303215.1.

14.2.6 Validating xlconfig.xml File

Before you start the upgrade process, ensure that the xlconfig.xml file at the location *$9.1.x.x_HOME*`/xellerate/config/xlconfig.xml` has the correct values for the parameters `DirectDb` and `MultiCastAddress`.

14.2.7 Creating Reconciliation Field of Type IT Resource

All account reconciliation Field Mapping configurations must have at least one Reconciliation field of type `IT Resource` defined. This can be done by adding a mapping from the Oracle Identity Manager Design Console. To do this, complete the following steps:

1. Create reconciliation field of type `IT Resource` by doing the following:
   a. Log in to the Oracle Identity Manager Design Console by running the following command from the location *ORACLE_HOME*`/designconsole/`:

      On UNIX: `./xlclient.sh`

      On Windows: `xlclient.cmd`

   b. Expand **Resource Management**.

c. Click **Resource Objects**.

d. Search for and select the Resource Object that you wish to modify.

e. Go to the **Object Reconciliation** tab.

f. Click **Add Field** under **Reconciliation Fields** tab.

g. Enter the Field Name, and select **IT Resource** as the **Field Type**.

h. Click Save icon.

2. Define mapping for the field `ITResource` by doing the following:

a. On the Oracle Identity Manager Design Console, expand **Process Management** on the left navigation pane.

b. Click **Process Definition**.

c. Go to the **Reconciliation Field Mapping** tab in the **Process Definition** form.

d. Search for the Resource Object.

e. Define mapping for the field **IT Resource**.

f. Save the form.

Note: This step is required if you are using connector for account reconciliation or if you wish to use connector for account reconciliation after you upgrade to 11.1.2.2.0.

14.3 Installing New Oracle Home and Upgrading Database Schemas

This section describes the tasks to be completed to upgrade the existing Oracle home and Database schemas.

This section includes the following topics:

- Creating the Necessary Schemas
- Installing Oracle WebLogic Server 10.3.6
- Installing Oracle SOA Suite 11.1.1.7.0 and Applying Mandatory SOA Patches
- Installing Oracle Identity Manager 11.1.2.2.0
- Upgrading Oracle Identity Manager Schema
- Upgrading Oracle Platform Security Services Schema
- Creating a Domain for Oracle Identity Manager 11.1.2.2.0
- Configuring Database Security Store
- Starting Administration Server and SOA Managed Server(s)

14.3.1 Creating the Necessary Schemas

Create the following schemas by using the Repository Creation Utility (RCU) 11.1.2.2.0:

- MDS schema for Oracle Identity Manager
- SOA schema
- MDS schema for Oracle SOA Suite

- OPSS schema
- ORASDPM schema

For information about creating schemas using Repository Creation Utility, refer to the following sections in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*:

- "Obtaining RCU"
- "Starting RCU"
- "Creating Schemas"

14.3.2 Installing Oracle WebLogic Server 10.3.6

Oracle Identity and Access Management 11.1.2.2.0 is certified with Oracle WebLogic Server 11*g* Release 1 (10.3.6). Therefore, you must install Oracle WebLogic Server 10.3.6.

To install Oracle WebLogic Server 10.3.6, do the following steps:

1. Download the WebLogic 10.3.6 Installer from Oracle Technology Network.

   For more information, see "Downloading the Installer From Oracle Technology Network" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the installer in graphical mode.

   For more information, see "Starting the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

14.3.3 Installing Oracle SOA Suite 11.1.1.7.0 and Applying Mandatory SOA Patches

Oracle Identity Manager 11.1.2.2.0 is certified with Oracle SOA Suite 11.1.1.7.0. Therefore, you must install Oracle SOA Suite 11.1.1.7.0.

For information about installing Oracle SOA Suite 11.1.1.7.0, see "Installing Oracle SOA Suite and Oracle Business Process Management Suite" in the *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

After you install SOA 11.1.1.7.0, you must apply mandatory SOA patches required for Oracle Identity Manager 11.1.2.2.0. For information about applying mandatory SOA patches, see "Mandatory Patches Required for Installing Oracle Identity Manager" in the *Oracle Fusion Middleware Release Notes*.

14.3.4 Installing Oracle Identity Manager 11.1.2.2.0

You must install Oracle Identity Manager 11.1.2.2.0 using the Oracle Identity and Access Management 11.1.2.2.0 installer.

For information about installing Oracle Identity Manager 11.1.2.2.0, see "Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0)" *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

14.3.5 Upgrading Oracle Identity Manager Schema

You must upgrade the existing Oracle Identity Manager schema to 11.1.2.2.0 using the Upgrade Assistant. To do this, complete the following steps:

1. Run the following command from the location *MW_HOME*/*OIM_HOME*/bin to launch the Upgrade Assistant:

   On UNIX: `./ua`

   On Windows: `ua.bat`

2. The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed.

   Click **Next**.

3. The **Specify Operation** screen is displayed.

   Select **Upgrade Oracle Identity Manager Schema**.

   Click **Next**.

4. The **Prerequisite** screen is displayed.

   Select the following check boxes:

   - **Database Schema backup completed**: Ensure that you have backed up your Oracle Identity Manager repositories on the database before upgrading. The Upgrade Assistant does not verify that the repositories have been backed up, so this option serves as a reminder.
   - **Database version is certified by Oracle for Fusion Middleware upgrade**: The Upgrade Assistant requires that the Oracle Data Integrator repositories reside on a supported database. For more information about the Database requirements, see Oracle Fusion Middleware System Requirements and Specifications.
   - **OSI Data Upgrade Performed**: Ensure that you have upgraded OSI data as described in Section 14.2.5, "Upgrading the OSI Data".

   Click **Next**.

5. The **Specify OIM Database** screen is displayed.

   Specify the following details:

   - **Host**: Enter the name of the host where database is running.
   - **Port**: Enter the port number for the host running database. The default port number for Oracle databases is `1521`.
   - **Service Name**: Specify the service name for the database. Typically, the service name is the same as the global database name.
   - **OIM Schema**: Specify the Oracle Identity Manager schema name.
   - **SYS Password**: Enter the password of the `SYS` user.

   Click **Next**.

6. The **Examining Components** screen is displayed.

   Click **Next**.

7. The **Upgrade Summary** screen is displayed.

   Click **Upgrade**.

8. The **Upgrade Progress** screen is displayed. This screen provides the following information:

   - The status of the upgrade
   - Any errors or problems that occur during the upgrade

Click **Next**.

9. The **Upgrade Complete** screen is displayed. This screen confirms that the upgrade was complete. The Upgrade Assistant generates log file at the location *OIM_HOME*/upgrade/logs/ua*Timestamp*.log. Check the log file for any errors or warnings.

   Click **Close**.

14.3.6 Upgrading Oracle Platform Security Services Schema

After you upgrade Oracle Identity Manager schema, you must upgrade the Oracle Platform Security Services schema using Patch Set Assistant. To do this, complete the following steps:

1. Start the Patch Set Assistant from the location $*ORACLE_HOME*/bin using the following command:

   ```
   ./psa
   ```

2. Select **opss**.

3. Specify the Database connection details, and select the schema to be upgraded.

For more information about upgrading schemas using Patch Set Assistant, see Section 2.6, "Upgrading Schemas Using Patch Set Assistant".

After you upgrade Oracle Platform Security Services schema, verify the upgrade by checking the log file at the location *MW_HOME*/oracle_common/upgrade/logs/psa<*timestamp*>.log. The *timestamp* refers to the actual date and time when Patch Set Assistant was run. If the upgrade fails, check the log files to rectify the errors and run the Patch Set Assistant again.

Also follow the instructions described in Section 2.6.4, "Verifying Schema Upgrade" to verify the Oracle Platform Security Services schema upgrade.

14.3.7 Creating a Domain for Oracle Identity Manager 11.1.2.2.0

Create a WebLogic domain for Oracle Identity Manager 11.1.2.2.0 by running the configuration wizard from the Oracle Identity Manager 11.1.2.2.0 home.

For information about configuring Oracle Identity Manager 11.1.2.2.0, see "Creating a new WebLogic Domain for Oracle Identity Manager and SOA" *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

14.3.8 Configuring Database Security Store

After you create a domain for Oracle Identity Manager 11.1.2.2.0, you must configure the database security store for the Oracle Identity Manager 11.1.2.2.0 domain.

For information about configuring database security store, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

14.3.9 Starting Administration Server and SOA Managed Server(s)

Note: Do not start the Oracle Identity Manager Managed Server(s).

After you configure the database security store, start the WebLogic Administration Server and the SOA Managed Server(s).

For more information about starting the servers, see Section 2.9, "Starting the Servers".

14.4 Configuring Other Oracle Identity Manager Installed Components

This section describes how to configure other Oracle Identity Manager installed components like Oracle Identity Manager 11.1.2.2.0 Server.

This section includes the following topics:

- Configuring Oracle Identity Manager Server 11.1.2.2.0
- Restarting the Administration Server and SOA Managed Server

14.4.1 Configuring Oracle Identity Manager Server 11.1.2.2.0

You must configure the Oracle Identity Manager 11.1.2.2.0 Server using the configuration wizard. For information about configuring Oracle Identity Manager Server, see "Configuring Oracle Identity Manager Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Note: When configuring Oracle Identity Manager Server 11.1.2.2.0, ensure that you do not select the **Enable LDAP Sync** option on the Oracle Identity Manager Configuration Wizard. LDAP Sync should not be enabled or picked up as an option while upgrading. It can be enabled post upgrade after system verification and other post upgrade steps are completed.

14.4.2 Restarting the Administration Server and SOA Managed Server

To restart the Administration Server and SOA Managed Servers, you must stop them first and start them again in the following order:

1. Stop the SOA Managed Server(s).
2. Stop the WebLogic Administration Server.
3. Start the WebLogic Administration Server.
4. Start the SOA Managed Server(s).

For more information about stopping the servers, see Section 2.8, "Stopping the Servers".

For more information about starting the servers, see Section 2.9, "Starting the Servers".

14.5 Upgrading Oracle Identity Manager 9.1.x.x Middle Tier

This section describes the tasks to be completed to upgrade the Oracle Identity Manager middle tier.

This section includes the following topics:

- Starting and Stopping Oracle Identity Manager Managed Server(s)
- Upgrading the Oracle Identity Manager Middle Tier
- Restarting all the Servers

14.5.1 Starting and Stopping Oracle Identity Manager Managed Server(s)

Before you start upgrading the Oracle Identity Manager 9.1.x.x middle tier, you must start and stop the Oracle Identity Manager Managed Server(s).

For information about starting the Oracle Identity Manager Managed Server, see Section 2.9.3, "Starting the Managed Server(s)".

For information about stopping the Oracle Identity Manager Managed Server, see Section 2.8.1, "Stopping the Managed Server(s)".

14.5.2 Upgrading the Oracle Identity Manager Middle Tier

Upgrade the Oracle Identity Manager middle tier using the Upgrade Assistant. To do this, complete the following steps:

1. Run the following command from the location *MW_HOME*/*OIM_HOME*/bin to launch the Upgrade Assistant.

   On UNIX: `./ua -invPtrLoc $OIM_HOME/oraInst.loc`

   On Windows: `ua.bat -invPtrLoc $OIM_HOME\oraInst.loc`

2. The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed.

   Click **Next**.

3. The **Specify Operation** screen is displayed.

   Select **Upgrade Oracle Identity Manager Middle Tier**.

   Click **Next**.

4. The **Specify Source Directory** screen is displayed.

   Click **Browse** and enter the directory location of your Oracle Identity Manager 9.1 installation.

   Click **Next**.

5. The **Specify OIM Database** screen is displayed.

   Enter the following information:

   - **Host**: Enter the name of the host where the database resides.
   - **Port**: Enter the listening port of the database. For example, `1521`.
   - **Service Name**: Enter the service name of the database. Note that the service name typically consists of the system identifier (SID) and the network domain address of the database.
   - **OIM Schema**: Enter the name of the Oracle Identity Manager 9.1.x.x schema that resides in the database.
   - **SYS Password**: Enter the password for the `SYS` database account of the database that hosts the Oracle Identity Manager 9.1.x.x schema. The Upgrade Assistant needs these login credentials to connect to the database and read the contents of the Oracle Identity Manager schema.

   Click **Next**.

6. The **Specify MDS Database** screen is displayed.

   Enter the following information:

   - **Host**: Enter the name of the host computer where the database resides.

- **Port**: Enter the listening port of the database; for example, `1521`.
- **Service Name**: Enter the service name of the database. Note that the service name typically consists of the system identifier (SID) and the network domain address of the database.
- **SYS Password**: Enter the password of the database SYS user. The Upgrade Assistant needs these login credentials to connect to the database and read the contents of the MDS schema.

Click **Next**.

7. The **Specify MDS Schema** screen is displayed.

   Complete the following:

   - Select the MDS schemas from the drop-down menu.
   - Enter the password for the schema in the **Password** field. This password is required so that the Upgrade Assistant can upgrade and modify the schema. This is the Oracle MDS schema password that you set in the Repository Creation Utility (RCU) when you installed the schema in the database.

   Click **Next**.

8. The **Specify WebLogic Server** screen is displayed.

   Enter the following information:

   - **Host**: The host where the Oracle WebLogic Server domain resides.

     Ensure to include the full host name; for example:

     ```
     IDMHost1.example.com
     ```

   - **Port**: The listening port of the administration server. Typically, the administration server listens on port `7001`.
   - **Username**: The user name that is used to log in to the Administration Server. This is the same username you use to log in to the Administration Console for the domain.
   - **Password**: The password for the administrator account that is used to log in to the administration server. This is the same password you use to log in to the Administration Console for the domain.

   Click **Next**.

9. The **Specify SOA Server** screen is displayed.

   Enter the following information:

   - **Host**: The host where the SOA Managed Server resides.
   - **Port**: The listening port of the SOA Managed Server.
   - **Username**: The user name that is used to log in to the SOA Managed Server. This is the same username you use to log in to the Administration Console for the domain.
   - **Password**: The password for the administrator account that is used to log in to the SOA Managed Server. This is the same password you use to log in to the Administration Console for the domain.

   Click **Next**.

10. The **Specify Upgrade Options** screen is displayed.

Click **Next**.

> **Note:** This screen has an option **Start destination components after successful upgrade** to start all the servers after successful upgrade; However, Oracle Identity Manager does not support the option of starting destination components after successful upgrade.

The **Examining Components** screen is displayed.

Click **Next**.

11. The **Upgrade Summary** screen is displayed.

    Click **Upgrade**.

12. The **Upgrade Progress** screen is displayed. This screen provides the following information:

    - The status of upgrade
    - Any errors or problems that occur during the upgrade

    Click **Next**.

13. The **Upgrade Complete** screen is displayed. This screen confirms that the upgrade was complete.

    Click **Close**.

    The middle tier upgrade summary report is generated at the location *OIM_HOME*/upgrade/logs/oimUpgradeReportDir. This report gives detail on the feature name, its upgrade status and feature related report. Verify this report to ensure that the middle tier upgrade was successful.

14. Verify the middle tier upgrade as described in Verifying the Middle Tier Upgrade.

Verifying the Middle Tier Upgrade

Middle tier upgrade utility creates log file and HTML reports with upgrade details for feature. To verify that the Oracle Identity Manager middle tier upgrade was successful, verify the log file oimUpgradeReportDir generated at the location *OIM_HOME*/upgrade/logs. Also, review the HTML upgrade reports generated at the location *OIM_HOME*/upgrade/logs/oimUpgradeReportDir. The index.html report in this directory lists all the features upgraded during the middle tier upgrade.:

14.5.3 Restarting all the Servers

After you upgrade the Oracle Identity Manager middle tier, you must restart the WebLogic Administration Server, Oracle Identity Manager Managed Server(s), and the SOA Managed Server(s).

To restart the servers, you must stop the servers first and start them again in the following order:

1. Stop the SOA Managed Server(s).
2. Stop the WebLogic Administration Server.
3. Start the WebLogic Administration Server.
4. Start the SOA Managed Server(s).
5. Start the Oracle Identity Manager Managed Server(s).

For more information about stopping the servers, see Section 2.8, "Stopping the Servers".

For more information about starting the servers, see Section 2.9, "Starting the Servers".

14.6 Post-Upgrade Steps

This section describes the tasks that you need to perform after you upgrade Oracle Identity Manager 9.1.x.x to Oracle Identity Manager 11.1.2.2.0.

This section includes the following topics:

- Optional: Configuring the Oracle Identity Manager Design Console 11.1.2.2.0
- Optional: Configuring the Oracle Identity Manager Remote Manager 11.1.2.2.0
- Performing Post-Upgrade Tasks
- Verifying the Upgrade

14.6.1 Optional: Configuring the Oracle Identity Manager Design Console 11.1.2.2.0

If you wish to configure Oracle Identity Manager Design Console 11.1.2.2.0, follow the instructions described in the section "Optional: Configuring Oracle Identity Manager Design Console" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

14.6.2 Optional: Configuring the Oracle Identity Manager Remote Manager 11.1.2.2.0

If you wish to configure Oracle Identity Manager Remote Manager 11.1.2.2.0, follow the instructions described in the section "Optional: Configuring Oracle Identity Manager Remote Manager" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

14.6.3 Performing Post-Upgrade Tasks

After you upgrade Oracle Identity Manager 9.1.x.x to 11.1.2.2.0, you must perform the following mandatory post-upgrade tasks:

- Reviewing Performance Tuning Recommendations
- Running the Entitlement List Schedule
- Running the Entitlement Assignments Schedule Job
- Running the Evaluate User Policies Scheduled Task
- Running Catalog Synchronization
- UMS Notification Provider
- Upgrading User UDF
- Upgrading Application Instances
- Redeploying XIMDD
- Redeploying SPML-DSML
- Customizing Event Handlers
- Recompiling Adapters
- Rewriting Prepopulate Adapters

- Disabling User Login
- Upgrading Oracle Identity Management Reports
- Creating New SOA Composites
- Configuring Auto-Approval for Self-Registration
- Generating an Audit Snapshot
- Enabling Audit
- Creating Password Policies
- Reviewing OIM Data Purge Job Parameters
- Reviewing Connector Certification
- Verifying the Functionality of Connectors

14.6.3.1 Reviewing Performance Tuning Recommendations

After you upgrade to Oracle Identity Manager 11.1.2.2.0, you must review the Oracle Identity Manager specific performance tuning recommendations described in "Oracle Identity Manager Performance Tuning" in the *Oracle Fusion Middleware Performance and Tuning Guide*.

14.6.3.2 Running the Entitlement List Schedule

You must run the Entitlement List Schedule task in order to use catalog features.

Complete the following steps to run the Entitlement List Schedule job:

1. Log in to the following location:

   `http://<OIM_HOST>:<OIM_PORT>/sysadmin`

2. Click **System Management**.
3. Select **Scheduler**.
4. Enter "Entitlement List" in the **Search Scheduled Jobs** field and click **Search**.
5. Select **Entitlement List**.
6. Click **Run Now**. Wait till the job is complete.

14.6.3.3 Running the Entitlement Assignments Schedule Job

You must run the Entitlement Assignments schedule task in order to ensure that the existing entitlement grants are shown properly in the **My Entitlements** tab. Complete the following steps to run the Entitlement Assignments schedule job:

1. Log in to the following location:

   `http://<OIM_HOST>:<OIM_PORT>/sysadmin`

2. Click **System Management**.
3. Select **Scheduler**.
4. Enter `Entitlement Assignments` in the **Search Scheduled Jobs** field, and click **Search**.
5. Select **Entitlement Assignments**.
6. Click **Run Now**. Wait till the job is complete.

14.6.3.4 Running the Evaluate User Policies Scheduled Task

You must run the Evaluate User Policies scheduled task to start provisioning based on access policy after the role grant. This scheduled task can be configured to run every 10 minutes, or you can run this scheduled task manually.

To start the scheduler, see "Starting and Stopping the Scheduler" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

14.6.3.5 Running Catalog Synchronization

Resource objects are transformed during the upgrade process. In order to provision the resource of an object, called App instance, with Oracle Identity Manager 11.1.2.2.0, you must run the Catalog Synchronization job.

For more information, see "Bootstrapping the Catalog" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

Note: If no Entitlements show up, make sure that the Entitlements field in the child tables is set to `Entitlement=true`.and reloaded into the parent form. After setting `Entitlement=true`, regenerate the view and run the Entitlement List scheduler job.

14.6.3.6 UMS Notification Provider

This is a new Oracle Identity Manager 11.1.2.2.0 feature for notification. If you want to use this new notification model, after upgrading to 11.1.2.2.0, complete the following steps:

1. Configure Email driver from Enterprise Manager user interface:
   a. Log in to Oracle Enterprise Manager Fusion Middleware Control and do the following:

      i. Expand **Application Deployments**.

      ii. Expand **User Messaging Service**.

      iii. Select **usermessagingdriver-email (<soa_server1>)**.

      iv. Select **Email Driver Properties**.

      v. Select **in Driver-Specific Configuration**.

   b. Configure the values, as listed in Table 14–6:

Table 14–6 UMS Parameters and Description

Parameter	Description
OutgoingMailServer	Name of the SMTP server. For example: `abc.example.com`
OutgoingMailServerPort	Port of the SMTP server. For example: 456
OutgoingMailServerSecurity	The security setting used by the SMTP server Possible values can be None/TLS/SSL.

Table 14–6 (Cont.) UMS Parameters and Description

Parameter	Description
OutgoingUsername	Provide a valid username. For example: `abc.eg@example.com`
OutgoingPassword	Complete the following: 1. Select **Indirect Password**. Create a new user. 2. Provide a unique string for indirect **Username/Key**. For example: `OIMEmailConfig`. This mask the password and prevent it from exposing it in cleartext, in the config file. 3. Provide valid password for this account.

2. Configure the Notification provider XML through the Enterprise Manager user interface:
   a. Log in to Enterprise Manager and do the following:
      i. Expand **Application Deployments**.
      ii. Select **OIMAppMetadata(11.1.1.3.0)(oim_server1)** and right-click.
      iii. Select **System MBean Browser**.
      iv. Expand **Application Defined MBeans**.
      v. Expand **oracle.iam**.
      vi. Expand **Server_OIM_Server1**
      vii. Expand **Application: oim**.
      viii. Expand **IAMAppRuntimeMBean**.
      ix. Select **UMSEmailNotificationProviderMBean**.
   b. Configure the values, as listed in Table 14–7:

Table 14–7 Parameter for Configuring Notification Provider

Parameter	Description
Web service URL	Start the URL of UMS web service. Any SOA server can be used. For example: `http://<SOA_host>:<SOA_Port>/ucs/messaging/webservice`
Policies	The OWSM Policy is attached to the given web service, leave it blank.
Username	The username is given in the security header of web service. If there is no policy attached, leave it blank.
Password	The password given in the security header of web service. If there is no policy attached, leave it blank.

After upgrading to 11.1.2.2.0, if you want to use SMTP notification provider instead of the default UMS notification provider, do the following:

1. Log in to Enterprise Manager and do the following:

a. Expand **Application Deployments**.

b. Select **OIMAppMetadata(11.1.1.3.0)(oim_server1)** and Right click.

c. Select **System MBean Browser**.

d. Expand **Application Defined MBeans**.

e. Expand **oracle.iam**.

f. Expand **Server_OIM_Server1**

g. Expand **Application: oim**.

h. Expand **IAMAppRuntimeMBean**.

i. Select **UMSEmailNotificationProviderMBean**.

2. Ensure that the value of the attribute `Enabled` is set to `true`.

3. Provide the configuration values in MBean (username, password, mailServerName) or the name of IT Resource in MBean.

   The IT Resource name is the name given in `XL.MailServer` system property, before you upgrade Oracle Identity Manager 9.1.x.x to Oracle Identity Manager 11.1.2.2.0.

14.6.3.7 Upgrading User UDF

You must have UDF in your environment because if you do not update your User Interface with UDFs, several features like user creation, role creation, and self registration request where UDFs are involved fails.

This section contains the following topics:

- Rendering the UDFs
- User Interface Customization for 9.1.x.x Mandatory UDF and OOTB Attributes
- Lookup Query Modification

14.6.3.7.1 Rendering the UDFs For an Oracle Identity Manager 11.1.2.2.0 environment that has been upgraded from Oracle Identity Manager 9.1.x.x, the custom attributes for user entity already exist in the back-end. These attributes are not present as form fields on the Oracle Identity Manager 11.1.2.2.0 user interface screens until the user screens are customized to add the custom fields.

However, before you can customize the screens, you must first complete upgrading the custom attributes using the Upgrade User Form link in the System Administration console.

After completing the Upgrade User Form, the User value object (VO) instances in various Data Components like DataComponent-Catalog, DataComponent-My Information, DataComponent-User Registration shows the custom attributes. This includes all custom attributes available for Web Composer (Customized) and can be added to User user interface screens.

For more information, see "Customizing the Interface" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Complete the following steps to render UDFs:

1. Log in to the **Identity System Administration** console.

2. Click **Sandboxes**. Click **Create Sandbox**. A Create Sandbox window appears.

3. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.

4. Go to **Upgrade**. Select **Upgrade User Form**. Click **Upgrade Now**.

   Note: If you encounter any error popup or `ERROR/WARNING` level logs after clicking **Upgrade Now** button, you must analyze the error, and then export the sandbox for analysis and discard (Delete) the sandbox.

5. Publish the Sandbox.
6. Log out from Identity System Administration console.
7. Log in to **Identity Self Service** console.
8. Click **Create Sandbox**. A **Create Sandbox** window appears.
9. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
10. From the left navigation pane, select **Users**.
11. Click **Create User**. A **Create User** page opens. Fill up all the mandatory fields, and add UDFs. Add the same UDFs in **Modify User** and **User Detail** screen. Select the correct **Data Component** and **UserVO Name** as listed in Table 14–8.

    For example:

    From the left navigation pane, click **Users**. Click **User** to go to the **Create User** screen and fill all mandatory fields.
12. Click **Customize** on top right. Select **View**. Select **Source**.
13. Select **Name** in **Basic Information** and click **Edit** on the confirmation window.
14. Select **panelFormLayout**. Click **Add Content**.
15. Select the correct **Data Component** and **VO Name** as listed in Table 14–8:

Table 14–8 UDF Screens and Description

Screen Name	Data Component	VO Name	Procedure
Create User	Data Component - Catalog	UserVO	Do the following: 1. Click **User**. 2. Click **Create**, it launches the **Create User** screen.
Modify User	Data Component - Catalog	UserVO	Do the following: 1. Click **User** and search. 2. Select a single user from search results. 3. Click **Edit**, it launches the **Modify User** screen.
View User Details	Data Component - Manage Users	UserVO1	Do the following: 1. Click **User** and search. 2. Select a single user from search results.
Bulk Modify User Flow	Data Component - Catalog	UserVO	Do the following: 1. Click **User** and search. 2. Select more than a single user from search results.

Table 14–8 (Cont.) UDF Screens and Description

Screen Name	Data Component	VO Name	Procedure
My Information	Data Component - My Information	UserVO1	Do the following: 1. Click **Identity**. 2. Select the **My Information** sub-tab.
Customizing Search Results	Data Component - Manage Users	UserVO1	Do the following: 1. Click **Identity**. 2. Click **Users**. 3. Click **Customizations**, it opens the **Web Composer**.
User Registration	Data Component - User Registration	UserVO1	Do the following: 1. Click **Customize** to open **Web Composer**. 2. Enable the left navigation links for unauthenticated pages. 3. Click **User Registration**. 4. Select **User Registration**.
Adding UDF in Search Panel	NA	NA	Do the following: 1. Log in to Identity 2. Click **User**. 3. Search for "Add Fields" in the search box. It shows all searchable fields to the user.
Customizing Request Summary/Details	NA	NA	Requests created after Create User, Modify User, My Information, Self Registration

16. Click **Close**.
17. Click **Sandboxes**. Export the sandbox using **Export Sandbox.**
18. Publish the sandbox.
19. Log out from **Identity Self Service**, and log in again. The added UDF in the screen is seen.

> **Note:** You can upgrade and customize Role UDF and Organization UDF by following the instructions described in the table "Entities and Corresponding Data Components and View Objects" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

14.6.3.7.2 User Interface Customization for 9.1.x.x Mandatory UDF and OOTB Attributes If you have rendered the OOTB attributes as mandatory in Oracle Identity Manager 9.1.x.x, you must customize the user interface in order to achieve the same customizations after upgrade.

Note: First name is a required field for user creation and self resgistration. Even if the first name field is not marked as required field (*) in the user creation and self registration forms, you must still specify the first name during user creation and self registration, after you upgrade to 11.1.2.2.0.

To customize the user interface for mandatory UDF and OOTB attributes, do the following:

1. Log in to **Identity Self Service** console.
2. Click **Create Sandbox**. A **Create Sandbox** window appears.
3. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
4. From the left navigation pane, click **Users**. Click **User** to go to the **Create User** screen and fill all the mandatory fields.
5. Click **Customize** on top right. Select **View**. Select **Source**.
6. Select **Name** in **Basic Information** and click **Edit** on the confirmation window.
7. Select **panelFormLayout**. Click **Add Content**.
8. Click **Input Component** and click **Edit**.
9. On the Component Properties dialogue, select **Show Required** checkbox. In the Required field, select **Expression Editor**, and in the **Expression Editor** field, enter the value as **true**.
10. Click **Close**.
11. Click **Sandboxes**. Export the sandbox using **Export Sandbox.**
12. Publish the sandbox.
13. Log out from **Identity Self Service**, and log in again. The added UDF on the screen with an asterix (*) symbol is seen.

14.6.3.7.3 Lookup Query Modification In user customization upgrade, multiple values for the Save Column may exist in `User.xml`. Based on the possible values; single, multiple, and null, do the following in the upgraded environment:

- Use `Single` value for Save Column: User creation is successful, and the value of the field is also saved in database.
- Use `Multiple` or `NULL` value for Save Column: User creation is successful, but the value is not saved in database.

Recommendation

Update the **Lookup By Query** metadata definition attached to an attribute in User or Role through Config Service or Design Console.

14.6.3.8 Upgrading Application Instances

After you complete the upgrade, you must complete the following steps to upgrade Application Instances:

1. Log in to the following console:

   `http://<OIM_HOST>:<OIM_PORT>/sysadmin`

2. Expand **Upgrade** on the left navigation pane.

3. Click **Upgrade Application Instances**.
4. Click **Upgrade Now**.

This creates the U/I Forms and Datasets for the Application Instances, and seeds to MDS.

14.6.3.9 Redeploying XIMDD

> **Note:** This section is required only if the Diagnostic Dashboard services for AD Password Sync were deployed in 9.1.x.x and if your application is deployed in staging mode in 9.1.x.x.

Before you can re-deploy, you must undeploy XIMDD from the 9.1.x.x Oracle Identity Manager Managed Server or from the cluster. To do so, complete the following steps:

1. Log in to the WebLogic Server Administration console:

   `host:admin port/console`
2. If you are running in production mode, click **Lock and Edit**.
3. Click **Deployments**.
4. In the resulting list, look for **XIMDD**.
5. If they are running, select **XIMDD.**
6. Click **Delete**.
7. Activate the changes.

To redeploy, complete the following steps:

1. Log in to the WebLogic Server Administration console:

   `host:admin port/console`
2. Click **Lock & Edit**.
3. Click **Deployments**.
4. Click **Install**.
5. In the path, give the path for XIMDD.ear

   The default path is in the following location:

   On UNIX, `$<OIM_HOME>/server/webapp/optional`

   On Windows, `<OIM_HOME>\server\webapp\optional`
6. Select **XIMDD.ear**. Click **Next**.
7. Select **Install this deployment as an application**. Click **Next** .
8. In **Select deployment targets** page, select **oim server**. Click **Next**.
9. In the **Optional Setting** page, click **Finish**.
10. Click **Deployments**.
11. Select **XIMDD**. Click **Start**.
12. From the options, select **Service All Requests**.

14.6.3.10 Redeploying SPML-DSML

Note: This section is required only if the DSML web services for AD Password Sync were deployed in 9.1.x.x.

To redeploy SPML-DSML, you must first undeploy SPML-DSML from the 9.1.x.x Oracle Identity Manager Managed Server or from the cluster. To undeploy SPML-DSML, complete the following steps:

1. Log in to the WebLogic Server Administration console:

   `host:admin port/console`
2. If you are running in production mode, obtain the Lock in order to make updates.
3. Click **Deployments**.
4. In the resulting list, look for **spml**.
5. If they are running, select **spml.**
6. Click **Delete**.
7. Activate the changes.

To redeploy SPML-DSML, complete the following steps:

1. Log in to WebLogic Server Administration console through the following path:

   host:admin port/console
2. Click **Lock & Edit**.
3. Click **Deployments**.
4. Click **Install**.
5. In the path give the path for spml.ear

   The default path is in the following location:

   On UNIX, `$<OIM_HOME>/server/apps`

   On Windows, `<OIM_HOME>\server\apps`
6. Select **spml-dsml.ear**. Click **Next**.
7. Select **Install this deployment as an application**. Click **Next** .
8. In **Select deployment targets** page, select **oim server**. Click **Next**.
9. In the **Optional Setting** page, click **Finish**.
10. Click **Deployments**.
11. Select **spml**. Click **Start**.
12. From the options, select **Service All Requests**.

14.6.3.11 Customizing Event Handlers

If you have used any event handlers in Oracle Identity Manager 9.1.x.x, you must re-customize the event handler for Oracle Identity Manager 11.1.2.2.0.

For more information, see "Developing Custom Event Handlers" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

14.6.3.12 Recompiling Adapters

After you upgrade to Oracle Identity Management 11*g*, you must recompile the adapters as described in "Compiling Adapters" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*. Some of your adapters may fail to compile. You must identify and recompile the adapters as described in the note 1311574.1 note at https://support.oracle.com.

14.6.3.13 Rewriting Prepopulate Adapters

After you upgrade to Oracle Identity Management 11*g*, you must rewrite the prepopulate adapter as described in "Prepopulation of an Attribute Value During Request Creation" in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.

14.6.3.14 Disabling User Login

In Oracle Identity Manager 11.1.2.2.0, the User login field is not mandatory. You must disable the user login mandatory option by completing the following steps:

1. Export the following files to MDS:
   - `/metadata/iam-features-requestactions/model-data/CreateUserDataSet.xml`
   - `/metadata/iam-features-requestactions/model-data/SelfCreateUserDataset.xml`

   For information about exporting metadat files, see "Exporting Metadata Files to MDS" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
2. Open the file `CreateUserDataSet.xml` in a text editor. Search for `<AttributeReference name="User Login"..>`, and set `required="false"`.
3. Open the file `SelfCreateUserDataset.xml` in a text editor. Search for `<AttributeReference name="User Login"..>`, and set `required="false"`.
4. Import the files `CreateUserDataSet.xml` and `SelfCreateUserDataset.xml` back to MDS. For information about importing metadata files, see "Importing Metadata Files from MDS" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

14.6.3.15 Upgrading Oracle Identity Management Reports

If you have a configured Oracle Identity Management Reports in Oracle Identity Manager 9.1 then you must upgrade the reports as described in "Upgrading to 11*g* Release 1 (11.1.1)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for 11*g* Release 1 (11.1.1).

> **Note:** BI Publisher cannot be accessed through the Oracle Identity Manager Administrative and User Console. You must open BI Publisher explicitly to access the Oracle Identity Manager 11*g* reports.

14.6.3.16 Creating New SOA Composites

You must create new SOA composites for all the 9.1.x.x approval processes after you upgrade to 11.1.2.2.0. It is recommended that you create reusable SOA Composites that can be used as approval workflows for different operations and entities.

For information about creating new SOA composites, see "Creating New SOA Composites" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

14.6.3.17 Configuring Auto-Approval for Self-Registration

After upgrading from Oracle Identity Manager 9.1.x.x, the auto approval feature is disabled for Oracle Identity Manager 11*g*. You must enable auto-approval for self-registration as described in "Enabling Auto-Approval for Self Registration Requests" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

14.6.3.18 Generating an Audit Snapshot

You must generate an audit snapshot of the audit tables as described in "Generating an Audit Snapshot" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

14.6.3.19 Enabling Audit

The audit features will not be enabled after upgrade if it was not there in Oracle Identity Manager 9.1. You can enable audit as described in "Modifying System Properties" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

14.6.3.20 Creating Password Policies

When you upgrade Oracle Identity Manager 9.1.x.x to 11.1.2.2.0, a default password policy will be seeded at the TOP organization. As a result, any password policy rules created using the older password policy model in Oracle Identity Manager 9.1.x.x environment will not be supported. The upgrade utility does not migrate the password policies od Oracle Identity Manager 9.1.x.x to 11.1.2.2.0. If you had made any password policy customizations on the older password policy rules, you must create equivalent password policies using the newer password policy model, and attach it to the respective organization.

For information about creating password policies, see "Managing Password Policies" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

14.6.3.21 Reviewing OIM Data Purge Job Parameters

This post-upgrade task is optional.

While upgrading Oracle Identity Manager to 11.1.2.2.0, the `OIM Data Purge Job` will be seeded in `enabled` state. By default, it will purge platform data with a retention period of 1 day for complete orchestration. To enable purge of request, reconciliation, and provisioning task, you must revisit the `OIM Data Purge Job` parameters.

For information about the user-configurable attributes, see "Configuring Real-Time Purge and Archival" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

14.6.3.22 Reviewing Connector Certification

Before you upgrade your existing Oracle Identity Manager environments, you must verify if the version of the existing connector is supported for Oracle Identity Manager 11.1.2.2.0. For information about the supported connector versions for Oracle Identity Manager 11.1.2.2.0, refer to the sections "Certified Components" and "Usage Recommendation" in the respective *Connector Guide* in Oracle Identity Manager Identity Connectors Documentation Library.

If you are using 9.x connector or GTC connector, do the following:

- If the 9.x connector that you are using is supported, you can continue to use the existing connector.

- If the 9.x connector is not supported, you must upgrade the existing 9.x connector to the latest 11.x connector after you upgrade the Oracle Identity Manager server to 11.1.2.2.0.
- Verify the data in the `Lookup` populated through lookup reconciliation that the IT Resource Key & IT Resource name is pre-fixed for code & decode respectively. If not, you must upgrade the existing connector to the latest available connector after you upgrade Oracle Identity Manager server.

If you are using 11g connector, the connector upgrade is not required.

14.6.3.23 Verifying the Functionality of Connectors

After you upgrade Oracle Identity Manager to 11.1.2.2.0, complete the following steps to verify the functionality of connectors:

- Verify if Account and Entitlement Tagging are available on the process form. For the connectors to work with Oracle Identity Manager 11.1.2.2.0, you must complete the steps described in the section "Configuring Oracle Identity Manager 11.1.2 or Later" in the respective *Connector Guide*.
- Verify if the customizations made to the connectors are intact.
- Verify if the 11.1.2.2.0 related artifacts like UI Forms and Application Instances are generated.
- Ensure that all the operations of the connectors are working fine.
- If there are two or more IT Resource field in the process form, complete the steps described in the following My Oracle Support note:

  My Oracle Support document ID 1535369.1
- If there are any lookup query fields in the process form of the related connector, then you must customize the UI need to display the same. For more information, see 'Lookup Query' section in "General Customization Concepts" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

14.6.4 Verifying the Upgrade

To verify the Oracle Identity Manager upgrade, do the following:

1. Review the middle tier upgrade summary report at the location *`OIM_HOME`*`/upgrade/logs/oimUpgradeReportDir`. The `index.html` lists all the features upgraded during this process.
2. Install the Diagnostic Dashboard and run the following tests:
   - Oracle Database Connectivity Check
   - Account Lock Status
   - Data Encryption Key Verification
   - Scheduler Service Status
   - JMS Messaging Verification
   - SOA-Oracle Identity Manager Configuration Check
   - SPML Web Service
   - Test OWSM setup
   - Test SPML to Oracle Identity Manager request invocation

- SPML attributes to Oracle Identity Manager attributes
- Username Test

3. Use the following URL in a web browser to verify that Oracle Identity Manager 11.1.2.2.0 is running:

   `http://<oim_host>:<oim_port>/sysadmin`

   `http://<oim_host>:<oim_port>/identity`

   where

   <oim_host> is the hostname of the machine running the administration server.

   <oim_port> is the port number.

4. Use Fusion Middleware Control to verify that Oracle Identity Manager and any other Oracle Identity Management components are running in the Oracle Fusion Middleware environment.

Part IV

Upgrading Oracle Identity and Access Management High Availability Environments

This part includes the following chapters:

- Chapter 15, "Upgrading Oracle Access Manager High Availability Environments"
- Chapter 16, "Upgrading Oracle Adaptive Access Manager High Availability Environments"
- Chapter 17, "Upgrading Oracle Identity Manager High Availability Environments"
- Chapter 18, "Upgrading Oracle Entitlements Server High Availability Environments"
- Chapter 19, "Upgrading Oracle Privileged Account Manager High Availability Environments"

15

Upgrading Oracle Access Manager High Availability Environments

This chapter describes how to upgrade Access Manager (Access Manager) high availability environments to Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

> **Note:** Before proceeding, check if your existing Access Manager version is supported for high availability upgrade. For more information on supported starting points for high availability upgrade, see Section 1.5, "Supported Starting Points for Upgrading High Availability Environments".

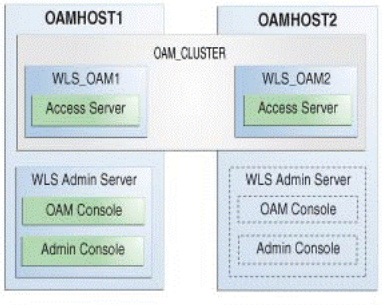
This chapter includes the following sections:

- Section 15.1, "Understanding Access Manager High Availability Upgrade Topology"
- Section 15.2, "Upgrade Roadmap"
- Section 15.3, "Shutting Down Administration Server and Managed Servers on OAMHOST1 and OAMHOST2"
- Section 15.4, "Backing Up the Existing Environment"
- Section 15.5, "Upgrading OAMHOST1 to 11.1.2.2.0"
- Section 15.6, "Updating Component Versions on OAMHOST1"
- Section 15.7, "Redeploying Access Manager Server Applications and Shared Libraries on OAMHOST1"
- Section 15.8, "Updating Binaries of WebLogic Server and Access Manager on OAMHOST2"
- Section 15.9, "Starting Administration Server and Managed Servers on OAMHOST1 and OAMHOST2"
- Section 15.10, "Troubleshooting"

15.1 Understanding Access Manager High Availability Upgrade Topology

Figure 15–1 shows the Access Manager cluster set up that can be upgraded to 11.1.2.2.0 by following the procedure described in this chapter.

Figure 15–1 Access Manager High Availability Upgrade Topology



On OAMHOST1, the following installations have been performed:

- An Access Manager instance has been installed in the WLS_OAM1 Managed Server.
- A WebLogic Server Administration Server has been installed. Under normal operations, this is the active Administration Server.

On OAMHOST2, the following installations have been performed:

- An Access Manager instance has been installed in the WLS_OAM2 Managed Server.
- A WebLogic Server Administration Server has been installed. Under normal operations, this is the passive Administration Server. You make this Administration Server active if the Administration Server on OAMHOST1 becomes unavailable.

The instances in the WLS_OAM1 and WLS_OAM2 Managed Servers on OAMHOST1 and OAMHOST2 are configured in a cluster named OAM_CLUSTER.

15.2 Upgrade Roadmap

Table 15–1 lists the steps to upgrade Access Manager high availability environment illustrated in Figure 15–1 to 11.1.2.2.0.

Table 15–1 Access Manager High Availability Upgrade Roadmap

Task No	Task	For More Information
1	Review the Access Manager high availability upgrade topology, and identify OAMHOST1 and OAMHOST2 on your setup.	See, Understanding Access Manager High Availability Upgrade Topology
2	Shut down the Administration Server and all the Managed Servers on OAMHOST1 and OAMHOST2.	See, Shutting Down Administration Server and Managed Servers on OAMHOST1 and OAMHOST2
3	Back up the existing environment.	See, Backing Up the Existing Environment
4	Upgrade OAMHOST1 to 11.1.2.2.0. This is the host with active Administration Server running on it.	See, Upgrading OAMHOST1 to 11.1.2.2.0
5	If your starting point is Oracle Access Manager 11*g* Release 1 (11.1.1.5.0), you must upgrade the packages oracle.dogwood.top and oracle.oam.server to 11.1.2.2.0 on OAMHOST1.	See, Updating Component Versions on OAMHOST1

Table 15–1 (Cont.) Access Manager High Availability Upgrade Roadmap

Task No	Task	For More Information
6	If you are upgrading Oracle Access Manager 11.1.1.5.0 environments, redeploy Access Manager Server applications and shared libraries on OAMHOST1 to target them to OAM_CLUSTER.	See, Redeploying Access Manager Server Applications and Shared Libraries on OAMHOST1
7	Update the binaries of Oracle WebLogic Server and Access Manager on OAMHOST2.	See, Updating Binaries of WebLogic Server and Access Manager on OAMHOST2
8	Start the WebLogic Administration Server and the Managed Servers on OAMHOST1 and OAMHOST2.	See, Starting Administration Server and Managed Servers on OAMHOST1 and OAMHOST2

15.3 Shutting Down Administration Server and Managed Servers on OAMHOST1 and OAMHOST2

Before you begin the upgrade process, you must stop the WebLogic Administration Server and all of the Access Manager Managed Servers on OAMHOST1 and OAMHOST2 in the following order:

1. Stop the Access Manager Managed Servers on both OAMHOST1 and OAMHOST2.
2. Stop the WebLogic Administration Server on OAMHOST1.

For information about stopping the Managed Server, see Section 2.8.1, "Stopping the Managed Server(s)".

For information about stopping the Administration Server, see Section 2.8.2, "Stopping the WebLogic Administration Server".

15.4 Backing Up the Existing Environment

After stopping all the servers, you must back up the following before proceeding with the upgrade process:

- *MW_HOME* directory (Middleware home directory), including the Oracle Home directories inside Middleware home on both OAMHOST1 and OAMHOST2.
- Access Manager Domain Home directory on both OAMHOST1 and OAMHOST2.
- Following Database schemas:
  - Oracle Access Manager schema
  - MDS schema
  - Audit and any other dependent schema

  For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

15.5 Upgrading OAMHOST1 to 11.1.2.2.0

In order to upgrade the Access Manager high availability environment to 11.1.2.2.0, you must first upgrade OAMHOST1 which has the active Administration Server. The

following are some of the important tasks involved in upgrading OAMHOST1 to 11.1.2.2.0:

- Upgrading Oracle WebLogic Server to 10.3.6.
- Upgrading the Access Manager binaries to 11.1.2.2.0.
- Upgrading the database schemas.
- Copying the modified domain mbean configurations.
- Upgrading the system configuration.

The procedure to upgrade OAMHOST1 depends on your starting point.

- If your starting point is Oracle Access Management Access Manager 11*g* Release 2 (11.1.2.1.0), follow the instructions described in Chapter 3, "Upgrading Oracle Access Manager 11g Release 2 (11.1.2.x.x) Environments" to upgrade OAMHOST1 to 11.1.2.2.0.
- If your starting point is Oracle Access Manager 11*g* Release 1 (11.1.1.5.0), follow the instructions described in Chapter 9, "Upgrading Oracle Access Manager 11g Release 1 (11.1.1.x.x) Environments" to upgrade OAMHOST1 to 11.1.2.2.0.

15.6 Updating Component Versions on OAMHOST1

If your starting point is Oracle Access Manager 11*g* Release 1 (11.1.1.5.0), you must upgrade the packages oracle.dogwood.top and oracle.oam.server from 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2.2.0) by running the domain updater utility (com.oracle.cie.domain-update_1.0.0.0.jar) on OAMHOST1. OAMHOST1 is the host on which Administration Server is running. This step updates the domain-info.xml.

Note: If your starting point is Access Manager 11*g* Release 2 (11.1.2.1.0) or 11*g* Release 2 (11.1.2), skip this task.

To upgrade the necessary Oracle Access Manager packages to 11.1.2.2.0, complete the following steps on OAMHOST1:

1. Go to the directory *$ORACLE_HOME*/oaam/upgrade. The domain updater utility com.oracle.cie.domain-update_1.0.0.0.jar file is located in this directory.
2. Upgrade the package oracle.dogwood.top 11.1.1.5.0 to 11.1.2.2.0 by running the following command:

   ```
   java -cp $MW_
   HOME/utils/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
   _1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <DOMAIN_HOME>
   oracle.dogwood.top:11.1.1.5.0,:11.1.2.2.0
   ```

   For example:

   ```
   java -cp
   /scratch/Oracle/Middleware/utils/config/10.3/config-launch.jar:./com.or
   acle.cie.domain-update_1.0.0.0.jar
   com.oracle.cie.external.domain.DomainUpdater
   /scratch/Oracle/Middleware/user_projects/domains/OAMDomain
   oracle.dogwood.top:11.1.1.5.0,:11.1.2.2.0
   ```

3. Upgrade the package oracle.oam.server 11.1.1.5.0 to 11.1.2.2.0 by running the following command:

```
java -cp $MW_
HOME/utils/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
_1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <DOMAIN_HOME>
oracle.oam.server:11.1.1.5.0,:11.1.2.2.0
```

For example:

```
java -cp
/scratch/Oracle/Middleware/utils/config/10.3/config-launch.jar:./com.or
acle.cie.domain-update_1.0.0.0.jar
com.oracle.cie.external.domain.DomainUpdater
/scratch/Oracle/Middleware/user_projects/domains/OAMDomain
oracle.oam.server:11.1.1.5.0,:11.1.2.2.0
```

15.7 Redeploying Access Manager Server Applications and Shared Libraries on OAMHOST1

On OAMHOST1, you must redeploy Access Manager server applications and shared libraries, and target the applications and shared libraries to OAM_CLUSTER, for the following reasons:

- To uptake new shared libraries that Access Manager server applications are dependent on.
- To uptake newer versions of Access Manager Administration and Managed Server applications.

For information about redeploying Access Manager server applications and shared libraries, see Section 9.16, "Redeploying Oracle Access Management Access Manager Servers and Shared Libraries".

Note: If you have already performed this task as part of Section 15.5, "Upgrading OAMHOST1 to 11.1.2.2.0", skip this section.

15.8 Updating Binaries of WebLogic Server and Access Manager on OAMHOST2

After you upgrade the Access Manager environment on OAMHOST1, you must update the binaries of Oracle WebLogic Server and Access Manager to 10.3.6 and 11.1.2.2.0 versions respectively on OAMHOST2 by completing the following tasks:

1. Updating Oracle WebLogic Server Binaries to 10.3.6
2. Updating Access Manager Binaries to 11.1.2.2.0

15.8.1 Updating Oracle WebLogic Server Binaries to 10.3.6

Oracle Identity and Access Management 11.1.2.2.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Identity Manager environment is using Oracle WebLogic Server 10.3.5 or the previous versions, you must update the Oracle WebLogic Server binaries to 10.3.6 by completing the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

For more information, see "Downloading an Upgrade Installer From My Oracle Support" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

   For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

15.8.2 Updating Access Manager Binaries to 11.1.2.2.0

To update the existing Access Manager binaries to Access Manager 11.1.2.2.0, you must use the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Installer. During the procedure, specify the location of your existing Middleware Home. This upgrades the Access Manager binaries 11.1.2.2.0.

For information about updating Access Manager binaries to 11.1.2.2.0, see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

15.9 Starting Administration Server and Managed Servers on OAMHOST1 and OAMHOST2

Start the WebLogic Administration Server and the Access Manager Managed Servers on `OAMHOST1` and `OAMHOST2` in the following order:

1. Start the WebLogic Administration Server on `OAMHOST1`.
2. Start the Access Manager Managed Servers on `OAMHOST1` and `OAMHOST2`.

For more information about starting the WebLogic Administration Server, see Section 2.9.2, "Starting the WebLogic Administration Server".

For more information about starting the Managed Servers, see Section 2.9.3, "Starting the Managed Server(s)".

15.10 Troubleshooting

This section describes troubleshooting methods for some of the common problems that might occur during the upgrade process.

> **Note:** For information about the issues that you might encounter during the upgrade process, and their workarounds, see *Oracle Fusion Middleware Release Notes*.

This section contains the following topics:

- Multi-Data Centre Feature Not Working After Upgrade

15.10.1 Multi-Data Centre Feature Not Working After Upgrade

If you had enabled Multi-Data Centre (MDC) feature in your 11.1.2.x.x setup, you must re-register the MDC partners and enable the MDC functionality that is added in 11.1.2.2.0. To do this, complete the following steps post-upgrade:

1. In each Data Centre (DC), remove the MDC partners by running the following WebLogic Scripting Tool (WLST) command:

```
removePartnerForMultiDataCentre("<cluster_ID>")
```

For example:

```
removePartnerForMultiDataCentre("cluster1")
```

You must run this command for each of the MDC partners. For more information about using the `removePartnerForMultiDataCentre()` command, see "removePartnerForMultiDataCentre" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

2. In 11.1.2.2.0, fail over for the MDC partners are supported. Therefore, you must specify the primary and secondary servers for each of the MDC partners using the Access Manager console. To do this, complete the following steps:

   a. Log in to the Access Manager 11.1.2.2.0 console using the following URL:

      `http://oam_admin_server_host:oam_admin_server_port/oamconsole`

   b. Navigate to **SSO Agents**.

   c. Modify the **Primary Server** and **Secondary Server** for each of the MDC partners.

3. Add the modified MDC partners to the respective Data Centres using the following command:

   ```
   addPartnerForMultiDataCentre(propfile="../MDC_
   properties/partnerInfo.properties")
   ```

   While running this command, make sure you use the updated `partnerInfo.properties` file. You must run this command for each of the MDC partners. For more information about using the `addPartnerForMultiDataCentre()` command, see "addPartnerForMultiDataCentre" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

4. Verify that the **MultiDataCenterPartners** section in each of the MDC partner profile contains the following settings instead of the Hostname and Port:

   ```
   <Setting Name="PrimaryHostPort" Type="xsd:string">
   <Setting Name="SecondaryHostPort" Type="xsd:string">
   ```

16

Upgrading Oracle Adaptive Access Manager High Availability Environments

This chapter describes how to upgrade Oracle Adaptive Access Manager high availability environments to 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

> **Note:** Before proceeding, check if your existing Oracle Adaptive Access Manager version is supported for high availability upgrade. For more information on supported starting points for high availability upgrade, see Section 1.5, "Supported Starting Points for Upgrading High Availability Environments".

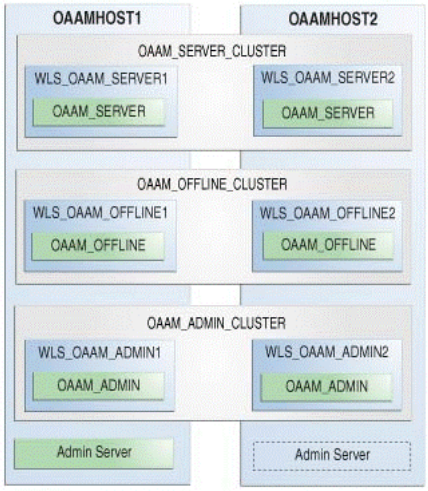
This chapter includes the following sections:

- Section 16.1, "Understanding Oracle Adaptive Access Manager High Availability Upgrade Topology"
- Section 16.2, "Upgrade Roadmap"
- Section 16.3, "Shutting Down Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2"
- Section 16.4, "Backing Up the Existing Environment"
- Section 16.5, "Updating Binaries of WebLogic Server and Oracle Adaptive Access Manager on OAAMHOST2"
- Section 16.6, "Upgrading OAAMHOST1 to 11.1.2.2.0"
- Section 16.7, "Starting Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2"

16.1 Understanding Oracle Adaptive Access Manager High Availability Upgrade Topology

Figure 16–1 shows the Oracle Adaptive Access Manager cluster set up that can be upgraded to 11.1.2.2.0 by following the procedure described in this chapter.

Figure 16–1 Oracle Adaptive Access Manager High Availability Upgrade Topology



The host `OAAMHOST1` contains the following:

- An Oracle Adaptive Access Manager Managed Server `WLS_OAAM_SERVER1` that hosts Oracle Adaptive Access Manager Server application (`OAAM_SERVER`).
- An Oracle Adaptive Access Manager Managed Server `WLS_OAAM_OFFLINE1` that hosts Oracle Adaptive Access Manager Offline Server application (`OAAM_OFFLINE`).
- An Oracle Adaptive Access Manager Managed Server `WLS_OAAM_ADMIN1` that hosts Oracle Adaptive Access Manager Admin application (`OAAM_ADMIN`).
- A WebLogic Server Administration Server. Under normal operations, this is the active Administration Server.

The host `OAAMHOST2` contains the following:

- An Oracle Adaptive Access Manager Managed Server `WLS_OAAM_SERVER2` that hosts Oracle Adaptive Access Manager Server application (`OAAM_SERVER`).
- An Oracle Adaptive Access Manager Managed Server `WLS_OAAM_OFFLINE2` that hosts Oracle Adaptive Access Manager Offline Server application (`OAAM_OFFLINE`).
- An Oracle Adaptive Access Manager Managed Server `WLS_OAAM_ADMIN2` that hosts Oracle Adaptive Access Manager Admin application (`OAAM_ADMIN`).
- A WebLogic Server Administration Server. Under normal operations, this is the passive Administration Server. You make this Administration Server active if the Administration Server on `OAAMHOST1` becomes unavailable.

The Oracle Adaptive Access Manager Managed Servers `WLS_OAAM_SERVER1` and `WLS_OAAM_SERVER2` hosting Oracle Adaptive Access Manager Server application on `OAAMHOST1` and `OAAMHOST2` are configured in a cluster named `OAAM_SERVER_CLUSTER`, to work in active-active mode.

The Oracle Adaptive Access Manager Managed Servers `WLS_OAAM_OFFLINE1` and `WLS_OAAM_OFFLINE2` hosting Oracle Adaptive Access Manager Offline Server application on `OAAMHOST1` and `OAAMHOST2` are configured in a cluster named `OAAM_OFFLINE_CLUSTER`, to work in active-active mode.

The Oracle Adaptive Access Manager Managed Servers `WLS_OAAM_ADMIN1` and `WLS_OAAM_ADMIN2` hosting Oracle Adaptive Access Manager Admin application on

OAAMHOST1 and OAAMHOST2 are configured in a cluster named OAAM_ADMIN_CLUSTER, to work in active-active mode.

16.2 Upgrade Roadmap

Table 16–1 lists the steps to upgrade Oracle Adaptive Access Manager high availability environment illustrated in Figure 16–1 to 11.1.2.2.0.

Table 16–1 Oracle Adaptive Access Manager High Availability Upgrade Roadmap

Task No	Task	For More Information
1	Review the Oracle Adaptive Access Manager high availability upgrade topology, and identify OAAMHOST1 and OAAMHOST2 on your setup.	See, Understanding Oracle Adaptive Access Manager High Availability Upgrade Topology
2	Shut down the Administration Server and all the Managed Servers on OAAMHOST1 and OAAMHOST2.	See, Shutting Down Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2
3	Back up the existing environment.	See, Backing Up the Existing Environment
4	Update the binaries of Oracle WebLogic Server and Oracle Adaptive Access Manager on OAAMHOST2.	See, Updating Binaries of WebLogic Server and Oracle Adaptive Access Manager on OAAMHOST2
5	Upgrade OAAMHOST1 to 11.1.2.2.0. This is the host with active Administration Server running on it.	See, Upgrading OAAMHOST1 to 11.1.2.2.0
6	Start the WebLogic Administration Server and the Managed Servers on OAAMHOST1 and OAAMHOST2.	See, Starting Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2

16.3 Shutting Down Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2

Before you begin the upgrade process, you must stop the WebLogic Administration Server and all of the Oracle Adaptive Access Manager Managed Servers on OAAMHOST1 and OAAMHOST2 in the following order:

1. Stop the Oracle Adaptive Access Manager Managed Servers on both OAAMHOST1 and OAAMHOST2.
2. Stop the WebLogic Administration Server on OAAMHOST1.

For information about stopping the Managed Server, see Section 2.8.1, "Stopping the Managed Server(s)".

For information about stopping the Administration Server, see Section 2.8.2, "Stopping the WebLogic Administration Server".

16.4 Backing Up the Existing Environment

After stopping all the servers, you must back up the following before proceeding with the upgrade process:

- *MW_HOME* directory (Middleware home directory), including the Oracle Home directories inside Middleware home on both OAAMHOST1 and OAAMHOST2.

- Oracle Adaptive Access Manager Domain Home directory on both `OAAMHOST1` and `OAAMHOST2`.
- Following Database schemas:
  - Oracle Adaptive Access Manager schema
  - IAU schema, if it is part of any of your Oracle Adaptive Access Manager schemas
  - MDS schema

  For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

16.5 Updating Binaries of WebLogic Server and Oracle Adaptive Access Manager on OAAMHOST2

Before you upgrade `OAAMHOST1` that hosts Administration Server, you must upgrade the binaries of Oracle WebLogic Server and Oracle Adaptive Access Manager to 10.3.6 and 11.1.2.2.0 versions respectively on `OAAMHOST2`. To do this, complete the following steps on `OAAMHOST2`:

1. Updating Oracle WebLogic Server Binaries to 10.3.6
2. Updating Oracle Adaptive Access Manager Binaries to 11.1.2.2.0

16.5.1 Updating Oracle WebLogic Server Binaries to 10.3.6

Oracle Identity and Access Management 11.1.2.2.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Identity Manager environment is using Oracle WebLogic Server 10.3.5 or the previous versions, you must update the Oracle WebLogic Server binaries to 10.3.6 by completing the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

   For more information, see "Downloading an Upgrade Installer From My Oracle Support" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

   For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

16.5.2 Updating Oracle Adaptive Access Manager Binaries to 11.1.2.2.0

To update the existing Oracle Adaptive Access Manager binaries to Oracle Adaptive Access Manager 11.1.2.2.0, you must use the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Installer. During the procedure, specify the location of your existing Middleware Home. This upgrades the Oracle Adaptive Access Manager binaries 11.1.2.2.0.

For information about updating Oracle Adaptive Access Manager binaries to 11.1.2.2.0, see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

16.6 Upgrading OAAMHOST1 to 11.1.2.2.0

After you upgrade the binaries of Oracle WebLogic Server and Oracle Adaptive Access Manager on `OAAMHOST2`, you must upgrade `OAAMHOST1` which has the active Administration Server. Upgrading `OAAMHOST2` to 11.1.2.2.0 includes the following important tasks:

- Upgrading Oracle WebLogic Server to 10.3.6.
- Upgrading the Oracle Adaptive Access Manager binaries to 11.1.2.2.0.
- Upgrading the database schemas.
- Upgrading Oracle Platform Security Services.
- Redeploying applications.

The procedure to upgrade `OAAMHOST1` depends on your starting point.

- If your starting point is Oracle Adaptive Access Manager 11*g* Release 2 (11.1.2.1.0), follow the instructions described in Chapter 4, "Upgrading Oracle Adaptive Access Manager 11g Release 2 (11.1.2.x.x) Environments" to upgrade `OAAMHOST1` to 11.1.2.2.0.
- If your starting point is Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0), follow the instructions described in Chapter 10, "Upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x) Environments" to upgrade `OAAMHOST1` to 11.1.2.2.0.

16.7 Starting Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2

Start the WebLogic Administration Server and the Oracle Adaptive Access Manager Managed Servers on `OAAMHOST1` and `OAAMHOST2` in the following order:

1. Start the WebLogic Administration Server on `OAAMHOST1`.
2. Start the Oracle Adaptive Access Manager Managed Servers on `OAAMHOST1` and `OAAMHOST2`.

For more information about starting the WebLogic Administration Server, see Section 2.9.2, "Starting the WebLogic Administration Server".

For more information about starting the Managed Servers, see Section 2.9.3, "Starting the Managed Server(s)".

17

Upgrading Oracle Identity Manager High Availability Environments

This chapter describes how to upgrade Oracle Identity Manager high availability environments to 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

> **Note:** Before proceeding, check if your existing Oracle Identity Manager version is supported for high availability upgrade. For more information on supported starting points for high availability upgrade, see Section 1.5, "Supported Starting Points for Upgrading High Availability Environments".

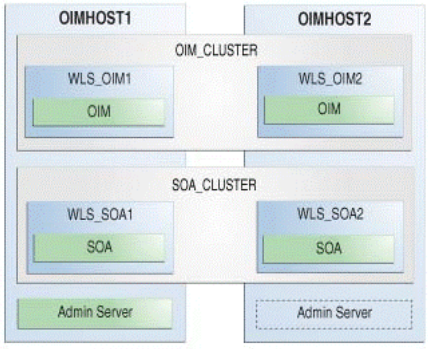
This chapter includes the following sections:

- Section 17.1, "Understanding Oracle Identity Manager High Availability Upgrade Topology"
- Section 17.2, "Upgrade Roadmap"
- Section 17.3, "Shutting Down Node Manager, Administration Server, and Managed Servers on OIMHOST1 and OIMHOST2"
- Section 17.4, "Backing Up the Existing Environment"
- Section 17.5, "Upgrading OIMHOST1 to 11.1.2.2.0"
- Section 17.6, "Updating Component Versions on OIMHOST1"
- Section 17.7, "Updating Binaries of WebLogic Server, Oracle Identity Manager, and Oracle SOA Suite on OIMHOST2"
- Section 17.8, "Replicating Domain Configuration on OIMHOST2"
- Section 17.9, "Upgrading Oracle Identity Manager Middle Tier on OIMHOST2"
- Section 17.10, "Starting Node Manager, Administration Server and Managed Servers on OIMHOST1 and OIMHOST2"
- Section 17.11, "Performing Post-Upgrade Tasks"
- Section 17.12, "Troubleshooting"

17.1 Understanding Oracle Identity Manager High Availability Upgrade Topology

Figure 17–1 shows the Oracle Identity Manager cluster set up that can be upgraded to 11.1.2.2.0 by following the procedure described in this chapter.

Figure 17–1 Oracle Identity Manager High Availability Upgrade Topology



On `OIMHOST1`, the following installations have been performed:

- An Oracle Identity Manager instance has been installed in the `WLS_OIM1` Managed Server and a SOA instance has been installed in the `WLS_SOA1` Managed Server.
- A WebLogic Server Administration Server has been installed. Under normal operations, this is the active Administration Server.

On `OIMHOST2`, the following installations have been performed:

- An Oracle Identity Manager instance has been installed in the `WLS_OIM2` Managed Server and a SOA instance has been installed in the `WLS_SOA2` Managed Server.
- A WebLogic Server Administration Server has been installed. Under normal operations, this is the passive Administration Server. You make this Administration Server active if the Administration Server on `OIMHOST1` becomes unavailable.

The instances in the `WLS_OIM1` and `WLS_OIM2` Managed Servers on `OIMHOST1` and `OIMHOST2` are configured as the `OIM_CLUSTER` cluster.

The instances in the `WLS_SOA1` and `WLS_SOA2` Managed Servers on `OIMHOST1` and `OIMHOST2` are configured as the `SOA_CLUSTER` cluster.

17.2 Upgrade Roadmap

Table 17–1 lists the steps to upgrade Oracle Identity Manager high availability environment illustrated in Figure 17–1 to 11.1.2.2.0.

Table 17–1 Oracle Identity Manager High Availability Upgrade Roadmap

Task No	Task	For More Information
1	Review the Oracle Identity Manager high availability upgrade topology, and identify `OIMHOST1` and `OIMHOST2` on your setup.	See, Understanding Oracle Identity Manager High Availability Upgrade Topology
2	Shut down the Administration Server, all the Managed Servers, and the Node Manager on `OIMHOST1` and `OIMHOST2`.	See, Shutting Down Node Manager, Administration Server, and Managed Servers on OIMHOST1 and OIMHOST2
3	Back up the existing environment.	See, Backing Up the Existing Environment
4	Upgrade `OIMHOST1` to 11.1.2.2.0. This is the host with active Administration Server running on it.	See, Upgrading OIMHOST1 to 11.1.2.2.0

Table 17–1 (Cont.) Oracle Identity Manager High Availability Upgrade Roadmap

Task No	Task	For More Information
5	If your starting point is Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0), you must upgrade the packages `oracle.dogwood.top` and `oracle.oim.suite` to 11.1.2.2.0 on `OIMHOST1`.	See, Updating Component Versions on OIMHOST1
6	Update the binaries of Oracle WebLogic Server, Oracle SOA Suite, and Oracle Identity Manager on `OIMHOST2`.	See, Updating Binaries of WebLogic Server, Oracle Identity Manager, and Oracle SOA Suite on OIMHOST2
7	Replicate the domain configuration of `OIMHOST1` on `OIMHOST2`. To do this, you must pack the domain on `OIMHOST1`, and unpack it on `OIMHOST2`.	See, Replicating Domain Configuration on OIMHOST2
8	On `OIMHOST2`, remove the file `setOIMDomainEnv.sh`, and upgrade the Oracle Identity Manager middle tier.	See, Upgrading Oracle Identity Manager Middle Tier on OIMHOST2
9	Start the Administration Server and the Managed Servers on `OIMHOST1` and `OIMHOST2`.	See, Starting Node Manager, Administration Server and Managed Servers on OIMHOST1 and OIMHOST2
10	Perform the necessary post-upgrade tasks.	See, Performing Post-Upgrade Tasks

17.3 Shutting Down Node Manager, Administration Server, and Managed Servers on OIMHOST1 and OIMHOST2

Before you begin the upgrade process, you must stop the WebLogic Administration Server, Node Manager, and all the Oracle Identity Manager and SOA Managed Servers on `OIMHOST1` and `OIMHOST2` in the following order:

1. Stop the Oracle Identity Manager Managed Server on both `OIMHOST1` and `OIMHOST2`.
2. Stop the SOA Managed Server on both `OIMHOST1` and `OIMHOST2`.
3. Stop the WebLogic Administration Server on `OIMHOST1`.
4. Stop the Node Manager on `OIMHOST1` and `OIMHOST2`.

For information about stopping the Managed Server, see Section 2.8.1, "Stopping the Managed Server(s)".

For information about stopping the Administration Server, see Section 2.8.2, "Stopping the WebLogic Administration Server".

For information about stopping Node Manager, see Section 2.8.3, "Stopping the Node Manager".

17.4 Backing Up the Existing Environment

After stopping all the servers, you must back up the following before proceeding with the upgrade process:

- *MW_HOME* directory (Middleware home directory), including the Oracle Home directories inside Middleware home on both OIMHOST1 and OIMHOST2.
- Domain Home directory on both OIMHOST1 and OIMHOST2.
- Following Database schemas:
  - Oracle Identity Manager schema
  - MDS schema
  - ORASDPM schema
  - SOAINFRA schemas
  - OPSS schema (only if you are upgrading 11.1.2.1.0 or 11.1.2 environments)

  For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

17.5 Upgrading OIMHOST1 to 11.1.2.2.0

In order to upgrade the Oracle Identity Manager high availability environment to 11.1.2.2.0, you must first upgrade OIMHOST1 which has the active Administration Server. The following are some of the important tasks involved in upgrading OIMHOST1 to 11.1.2.2.0:

- Performing pre-upgrade tasks like reviewing the changes in features of Oracle Identity Manager 11.1.2.2.0, reviewing system requirements and certifications, generating and analyzing the pre-upgrade report, performing necessary pre-upgrade tasks described in the report and so on.
- Upgrading Oracle Home and Database schemas which includes tasks like upgrading Oracle WebLogic Server, upgrading Oracle SOA Suite, updating Oracle Identity Manager binaries, upgrading Oracle Platform Security Services, upgrading Oracle Identity Manager schemas and so on.
- Upgrading the Oracle Identity Manager middle tier.
- Upgrading other Oracle Identity Manager installed components like Oracle Identity Manager Design Console and Oracle Identity Manager Remote manager.
- Performing any mandatory post-upgrade tasks.

The procedure to upgrade OIMHOST1 depends on your starting point.

- If your starting point is Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) or 11*g* Release 2 (11.1.2), follow the instructions described in Chapter 5, "Upgrading Oracle Identity Manager 11g Release 2 (11.1.2.x.x) Environments" to upgrade OIMHOST1 to 11.1.2.2.0.
- If your starting point is Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0), follow the instructions described in Chapter 11, "Upgrading Oracle Identity Manager 11g Release 1 (11.1.1.x.x) Environments" to upgrade OIMHOST1 to 11.1.2.2.0.

17.6 Updating Component Versions on OIMHOST1

If your starting point is Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0), you must upgrade the packages oracle.dogwood.top and oracle.oim.suite from 11*g* Release 1 (11.1.1.5.0) to 11*g* Release 2 (11.1.2.2.0) by running the domain updater utility (com.oracle.cie.domain-update_1.0.0.0.jar) on OIMHOST1. OIMHOST1 is the host on which Administration Server is running. This step updates the domain-info.xml.

Note: If your starting point is Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) or 11*g* Release 2 (11.1.2), skip this task.

To upgrade the necessary Oracle Identity Manager packages to 11.1.2.2.0, complete the following steps on `OIMHOST1`:

1. Go to the directory *`$ORACLE_HOME`*`/oaam/upgrade`. The domain updater utility `com.oracle.cie.domain-update_1.0.0.0.jar` file is located in this directory.
2. Upgrade the package `oracle.dogwood.top` 11.1.1.5.0 to 11.1.2.2.0 by running the following command:

   ```
   java -cp $MW_
   HOME/utils/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
   _1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <DOMAIN_HOME>
   oracle.dogwood.top:11.1.1.5.0,:11.1.2.2.0
   ```

   For example:

   ```
   java -cp
   /scratch/Oracle/Middleware/utils/config/10.3/config-launch.jar:./com.or
   acle.cie.domain-update_1.0.0.0.jar
   com.oracle.cie.external.domain.DomainUpdater
   /scratch/Oracle/Middleware/user_projects/domains/OIMDomain
   oracle.dogwood.top:11.1.1.5.0,:11.1.2.2.0
   ```

3. Upgrade the package `oracle.oim.suite` 11.1.1.5.0 to 11.1.2.2.0 by running the following command:

   ```
   java -cp $MW_
   HOME/utils/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
   _1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <DOMAIN_HOME>
   oracle.oim.suite:11.1.1.5.0,:11.1.2.2.0
   ```

   For example:

   ```
   java -cp
   /scratch/Oracle/Middleware/utils/config/10.3/config-launch.jar:./com.or
   acle.cie.domain-update_1.0.0.0.jar
   com.oracle.cie.external.domain.DomainUpdater
   /scratch/Oracle/Middleware/user_projects/domains/OIMDomain
   oracle.oim.suite:11.1.1.5.0,:11.1.2.2.0
   ```

17.7 Updating Binaries of WebLogic Server, Oracle Identity Manager, and Oracle SOA Suite on OIMHOST2

After you upgrade the Oracle Identity Manager environment on `OIMHOST1`, you must update the binaries of Oracle WebLogic Server, Oracle SOA Suite, and Oracle Identity Manager to 10.3.6, 11.1.1.7.0, and 11.1.2.2.0 versions respectively on `OIMHOST2` by doing the following:

1. Updating Oracle WebLogic Server Binaries to 10.3.6
2. Updating Oracle SOA Suite Binaries to 11.1.1.7.0
3. Updating Oracle Identity Manager Binaries to 11.1.2.2.0

17.7.1 Updating Oracle WebLogic Server Binaries to 10.3.6

Oracle Identity and Access Management 11.1.2.2.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Identity Manager environment is using Oracle WebLogic Server 10.3.5 or the previous versions, you must update the Oracle WebLogic Server binaries to 10.3.6 by completing the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

   For more information, see "Downloading an Upgrade Installer From My Oracle Support" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

   For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

17.7.2 Updating Oracle SOA Suite Binaries to 11.1.1.7.0

Oracle Identity Manager 11.1.2.2.0 is certified with Oracle SOA Suite 11g Release 1 (11.1.1.7.0). If you are not using Oracle SOA Suite 11.1.1.7.0, you must update your existing Oracle SOA Suite binaries to 11.1.1.7.0 by completing the steps:

1. Obtain the Oracle SOA Suite installer 11.1.1.7.0 installer from the location specified in the *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.
2. Start the Oracle SOA Suite 11.1.1.7.0 installer. For more information, see "Start the Installer" in the *Oracle Fusion Middleware Patching Guide*.
3. Update the Oracle SOA Suite binaries to 11.1.1.7.0 using the installer. For more information, see "Applying the Patch Set" in the *Oracle Fusion Middleware Patching Guide*.
4. Apply the mandatory Oracle SOA Suite patches required for Oracle Identity Manager 11.1.2.2.0. For more information, see "Mandatory Patches Required for Installing Oracle Identity Manager" in the *Oracle Fusion Middleware Release Notes*.

17.7.3 Updating Oracle Identity Manager Binaries to 11.1.2.2.0

To update the existing Oracle Identity Manager binaries to Oracle Identity Manager 11.1.2.2.0, you must use the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Installer. During the procedure, specify the location of your existing Middleware Home. This upgrades the Oracle Identity Manager binaries 11.1.2.2.0.

For information about updating Oracle Identity Manager binaries to 11.1.2.2.0, see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

17.8 Replicating Domain Configuration on OIMHOST2

You must replicate the domain configuration on `OIMHOST2`. This task involves packing the upgraded domain on `OIMHOST1` and unpacking it on `OIMHOST2`. To do this, complete the following steps:

1. On `OIMHOST1`, run the following command from the location *`$MW_HOME`*`/oracle_common/common/bin` to pack the upgraded domain:

   On UNIX:

```
sh pack.sh -domain=<Location_of_OIM_domain> -template=<Location_where_
domain_configuration_jar_to_be_created> -template_name="OIM Domain"
-managed=true
```

On Windows:

```
pack -domain=<Location_of_OIM_domain> -template=<Location_where_domain_
configuration_jar_needs_to_be_created> -template_name="OIM Domain"
-managed=true
```

2. Copy the domain configuration jar file created by the `pack` command on `OIMHOST1` to any accessible location on `OIMHOST2`.
3. On `OIMHOST2`, run the following command from the location *`$MW_HOME`*`/oracle_common/common/bin` to unpack the domain:

   On UNIX:

   ```
   sh unpack.sh -domain=<Location_of_OIM_domain> -template=<Location_on_
   OIMHOST2_where _you_copied_jar_file_created_by_pack_command>
   -overwrite_domain=true
   ```

   On Windows:

   ```
   unpack -domain=<Location_of_OIM_domain> -template=<Location_on_
   OIMHOST2_where _you_copied_jar_file_created_by_pack_command>
   -overwrite_domain=true
   ```

17.9 Upgrading Oracle Identity Manager Middle Tier on OIMHOST2

After you pack the domain on `OIMHOST1` and unpack it on `OIMHOST2`, you must remove the file `setOIMDomainEnv.sh` (on UNIX) or `setOIMDomainEnv.cmd` (on Windows) on `OIMHOST2`, and upgrade the Oracle Identity Manager middle tier on `OIMHOST2`. To do this, complete the following steps:

1. Go to the location *`$DOMAIN_HOME`*`/bin` on `OIMHOST2`.
2. Remove the file `setOIMDomainEnv.sh` (on UNIX) or `setOIMDomainEnv.cmd` (on Windows) by running the following command:

   On UNIX: `rm -rf setOIMDomainEnv.sh`

   On Windows: `del setOIMDomainEnv.cmd`

3. Upgrade the Oracle Identity Manager middle tier to 11.1.2.2.0 on `OIMHOST2` The procedure to upgrade Oracle Identity Manager middle tier depends on your starting point:

   - If your starting point is Oracle Identity Manager 11*g* Release 2 (11.1.2.1.0) or 11*g* Release 2 (11.1.2), follow the instructions described in Section 5.4, "Upgrading the Oracle Identity Manager Middle Tier" to upgrade Oracle Identity Manager middle tier to 11.1.2.2.0.
   - If your starting point is Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0), follow the instructions described in Section 11.3.11, "Upgrading Oracle Identity Manager Middle Tier" to upgrade Oracle Identity Manager middle tier.

17.10 Starting Node Manager, Administration Server and Managed Servers on OIMHOST1 and OIMHOST2

Start the Node Manager, WebLogic Administration Server, Oracle SOA Suite Managed Servers, and Oracle Identity Manager Managed Servers on `OIMHOST1` and `OIMHOST2` in the following order:

1. On `OIMHOST1` and `OIMHOST2`, start the Node Manager.
2. On `OIMHOST1`, start the WebLogic Administration Server.
3. On `OIMHOST1` and `OIMHOST2`, start the SOA Managed Servers.
4. On `OIMHOST1` and `OIMHOST2`, start the OIM Managed Servers.

For more information about starting the Node Manager, see Section 2.9.1, "Starting the Node Manager".

For more information about starting the WebLogic Administration Server, see Section 2.9.2, "Starting the WebLogic Administration Server".

For more information about starting the Managed Servers, see Section 2.9.3, "Starting the Managed Server(s)".

17.11 Performing Post-Upgrade Tasks

This section describes the post-upgrade tasks that you must perform after you upgrade Oracle Identity Manager high availability environments to 11.1.2.2.0. This section includes the following topics:

- Updating SOA Composites with OHS Attributes
- Updating SOA Config RMI URL for Oracle Identity Manager

17.11.1 Updating SOA Composites with OHS Attributes

After you upgrade Oracle Identity Manager 11*g* Release 2 (11.1.2) high availability environment to 11.1.2.2.0, the new SOA composites `DefaultOperationalApproval [3.0]` and `DefaultRequestApproval [3.0]` will be configured with the information of `OIMHOST2`. This can cause request approval malfunction. Therefore, you must update the SOA composites with the attributes of Oracle HTTP Server (OHS).

> **Note:** This task is required only if you are upgrading Oracle Identity Manager 11*g* Release 2 (11.1.2) to 11.1.2.2.0.

To update the SOA composites with the attributes of OHS, complete the following steps:

1. Log in to the Oracle Enterprise Manager Fusion Middleware Control Console using the following URL:

   `http://host:port/em`

2. Expand **SOA** on the left pane, select **soa-infra (WLS_SOA1)**, and then click **default**.
3. For the SOA composites **DefaultOperationalApproval [3.0]** and **DefaultRequestApproval [3.0]**, do the following:

   a. Click the composite name.

b. In the **Component Metrics**, click the composite type. For example, click **ApprovalTask** or **ChallengeTask**.

c. Go to the **Administration** tab, and update the following fields:

Host Name: Specify the host name of OHS.

HTTP Port: Is SSL mode, leave this field blank. If non-SSL mode, specify the OHS HTTP port.

HTTPS Port: If SSL mode, specify the OHS HTTPS port. If non-SSL mode, leave this field blank.

d. Click **Apply**.

17.11.2 Updating SOA Config RMI URL for Oracle Identity Manager

After you upgrade to Oracle Identity Manager 11*g* Release 1 (11.1.1.x.x) high availability environments to Oracle Identity Manager 11.1.2.2.0, you must check the SOA Config RMI URL. If it is empty, or if it is pointing to single Oracle SOA Suite server, then update the SOA Config RMI URL to point to the Oracle SOA Suite cluster (SOA_CLUSTER).

To do this, complete the following steps:

1. Log in to Oracle Enterprise Manager using the following URL:

   `http://host:port/em`

2. Select **Farm_IDMDomain** –> **Identity and Access** –> **OIM** –> **oim(*version*)**.
3. Select **MBean Browser** from the menu or right click to select it.
4. Select **Application defined Mbeans** –> **oracle.iam** –> **Server: wls_oim1** –> **Application: oim** –> **XML Config** –> **Config** –> **XMLConfig.SOAConfig** –> **SOAConfig**.
5. Change **SOA Config RMI URL** to `cluster:t3s://SOA_CLUSTER`.
6. Click **Apply**.

17.12 Troubleshooting

This section describes solutions to the common problems that you might encounter when upgrading Oracle Identity Manager high availability environments to 11.1.2.2.0.

> **Note:** For information about the issues that you might encounter during the upgrade process, and their workarounds, see *Oracle Fusion Middleware Release Notes*.

This section contains the following topic:

- Exception in Log When Creating Users

17.12.1 Exception in Log When Creating Users

After you upgrade Oracle Identity Manager 11.1.1.5.0 high availability environment to Oracle Identity Manager 11.1.2.2.0, you might see the following exception in the logs when you create users:

```
[2013-11-19T23:41:51.507-08:00] [oim_server1] [ERROR] []
```

```
[oracle.ods.virtualization.exception] [tid: UCP-worker-thread-19] [userId:
oiminternal] [ecid: 004utMMAEYz1VcP5Ifp2if00023p000Tdf,0] [APP:
oim#11.1.1.3.0] Could not initialize default mapping config[[
javax.xml.bind.UnmarshalException
 - with linked exception:
[java.io.FileNotFoundException:
/scratch/Oracle/Middleware/user_
projects/domains/IDMDomain/config/fmwconfig/ovd/oim/mappings.os_xml
(No such file or directory)
```

This does not cause the user creation task to fail. However, to eliminate this exception, you must manually copy the file `mappings.os_xml` from the location *`$MW_HOME`*`/oracle_common/modules/oracle.ovd_11.1.1/templates/mappings.os_xml` to the directory *`$DOMAIN_HOME`*`/config/fmwconfig/ovd/oim`.

18

Upgrading Oracle Entitlements Server High Availability Environments

This chapter describes how to upgrade Oracle Entitlements Server high availability environments to 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

> **Note:** Before proceeding, check if your existing Oracle Entitlements Server version is supported for high availability upgrade. For more information on supported starting points for high availability upgrade, see Section 1.5, "Supported Starting Points for Upgrading High Availability Environments".

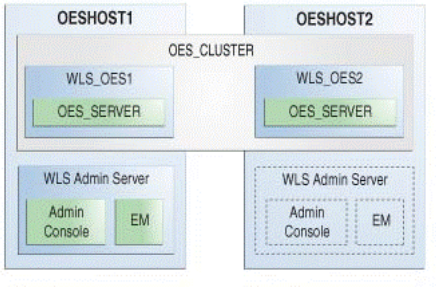
This chapter includes the following sections:

- Section 18.1, "Understanding Oracle Entitlements Server High Availability Upgrade Topology"
- Section 18.2, "Upgrade Roadmap"
- Section 18.3, "Shutting Down Administration Server and Managed Servers on OESHOST1 and OESHOST2"
- Section 18.4, "Backing Up the Existing Environment"
- Section 18.5, "Updating Binaries of WebLogic Server and Oracle Entitlements Server on OESHOST1"
- Section 18.6, "Upgrading Oracle Platform Security Services Schema on OESHOST1"
- Section 18.7, "Upgrading Oracle Platform Security Services on OESHOST1"
- Section 18.8, "Updating Binaries of WebLogic Server and Access Manager on OESHOST2"
- Section 18.9, "Redeploying APM Applications on OESHOST1 and OESHOST2"
- Section 18.10, "Starting Administration Server and Managed Servers on OESHOST1 and OESHOST2"

18.1 Understanding Oracle Entitlements Server High Availability Upgrade Topology

Figure 18–1 shows the Oracle Entitlements Server cluster set up that can be upgraded to 11.1.2.2.0 by following the procedure described in this chapter.

Figure 18–1 Oracle Entitlements Server High Availability Upgrade Topology



The host `OESHOST1` has the following installations:

- An Oracle Entitlements Server instance in the `WLS_OES1` Managed Server.
- A WebLogic Server Administration Server. Under normal operations, this is the active Administration Server.

The host `OAMHOST2` has the following installations:

- An Oracle Entitlements Server instance in the `WLS_OES2` Managed Server.
- A WebLogic Server Administration Server. Under normal operations, this is the passive Administration Server. You make this Administration Server active if the Administration Server on `OESHOST1` becomes unavailable.

The instances in the `WLS_OES1` and `WLS_OES2` Managed Servers on `OESHOST1` and `OESHOST2` are configured in a cluster named `OES_CLUSTER`.

18.2 Upgrade Roadmap

Table 18–1 lists the steps to upgrade Oracle Entitlements Server high availability environment illustrated in Figure 18–1 to 11.1.2.2.0.

Table 18–1 Oracle Entitlements Server High Availability Upgrade Roadmap

Task No	Task	For More Information
1	Review the Oracle Entitlements Server high availability upgrade topology, and identify `OESHOST1` and `OESHOST2` on your setup.	See, Understanding Oracle Entitlements Server High Availability Upgrade Topology
2	Shut down the Administration Server and all the Managed Servers on `OESHOST1` and `OESHOST2`.	See, Shutting Down Administration Server and Managed Servers on OESHOST1 and OESHOST2
3	Back up the Middleware home, Oracle home, and the Oracle Platform Security Services schema on `OESHOST1` and `OESHOST2`.	See, Backing Up the Existing Environment
4	Update the binaries of Oracle WebLogic Server and Oracle Entitlements Server on `OESHOST1`.	See, Updating Binaries of WebLogic Server and Oracle Entitlements Server on OESHOST1
5	Upgrade the Oracle Platform Security Services schema on `OESHOST1`.	See, Upgrading Oracle Platform Security Services Schema on OESHOST1
6	Upgrade Oracle Platform Security Services on `OESHOST1`.	See, Upgrading Oracle Platform Security Services on OESHOST1

Table 18–1 (Cont.) Oracle Entitlements Server High Availability Upgrade Roadmap

Task No	Task	For More Information
7	Update the binaries of Oracle WebLogic Server and Oracle Entitlements Server on OESHOST2.	See, Updating Binaries of WebLogic Server and Access Manager on OESHOST2
8	Redeploy the following APM applications on OESHOST1 and OESHOST2.	See, Redeploying APM Applications on OESHOST1 and OESHOST2
9	Start the WebLogic Administration Server and the Managed Servers on OESHOST1 and OESHOST2.	See, Starting Administration Server and Managed Servers on OESHOST1 and OESHOST2

18.3 Shutting Down Administration Server and Managed Servers on OESHOST1 and OESHOST2

Before you begin the upgrade process, you must stop the WebLogic Administration Server and all the Oracle Entitlements Server Managed Servers on OESHOST1 and OESHOST2 in the following order:

1. Stop the Oracle Entitlements Server Managed Servers on both OESHOST1 and OESHOST2.
2. Stop the WebLogic Administration Server on OESHOST1.

For information about stopping the Managed Server, see Section 2.8.1, "Stopping the Managed Server(s)".

For information about stopping the Administration Server, see Section 2.8.2, "Stopping the WebLogic Administration Server".

18.4 Backing Up the Existing Environment

After stopping all the servers, you must back up the following before proceeding with the upgrade process:

- *MW_HOME* directory (Middleware home directory), including the Oracle Home directories inside Middleware home on both OESHOST1 and OESHOST2.
- Oracle Entitlements Server Domain Home directory on both OESHOST1 and OAESHOST2.
- Oracle Platform Security Services schema

  For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

18.5 Updating Binaries of WebLogic Server and Oracle Entitlements Server on OESHOST1

After backing up the existing environment, you must update the binaries of Oracle WebLogic Server and Oracle Entitlements Server to 10.3.6 and 11.1.2.2.0 versions respectively on OESHOST1 by completing the following tasks:

1. Updating Oracle WebLogic Server Binaries to 10.3.6
2. Updating Oracle Entitlements Server Binaries to 11.1.2.2.0

18.5.1 Updating Oracle WebLogic Server Binaries to 10.3.6

Oracle Identity and Access Management 11.1.2.2.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Identity Manager environment is using Oracle WebLogic Server 10.3.5 or the previous versions, you must update the Oracle WebLogic Server binaries to 10.3.6 by completing the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

   For more information, see "Downloading an Upgrade Installer From My Oracle Support" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

   For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

18.5.2 Updating Oracle Entitlements Server Binaries to 11.1.2.2.0

To update the existing Oracle Entitlements Server binaries to Oracle Entitlements Server 11.1.2.2.0, you must use the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Installer. During the procedure, specify the location of your existing Middleware Home. This updates the Oracle Entitlements Server binaries 11.1.2.2.0.

For information about updating Oracle Entitlements Server binaries to 11.1.2.2.0, see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

18.6 Upgrading Oracle Platform Security Services Schema on OESHOST1

After updating the Oracle WebLogic Server and Oracle Entitlements Server binaries on `OESHOST1`, you must upgrade the Oracle Platform Security Services schema using Patch Set Assistant. To do this, complete the following steps on `OESHOST1`:

1. Start the Patch Set Assistant from the location *`$MW_HOME`*`/oracle_common/bin` using the following command:

   ```
   ./psa
   ```

2. Select **opss**.

3. Specify the Database connection details, and select the schema to be upgraded.

After you upgrade Oracle Platform Security Services schema, verify the upgrade by checking the log file at the location *`MW_HOME`*`/oracle_common/upgrade/logs/psa<`*`timestamp`*`>.log`.

The *`timestamp`* refers to the actual date and time when Patch Set Assistant was run. If the upgrade fails, check the log files to rectify the errors and run the Patch Set Assistant again.

For more information about upgrading schemas using Patch Set Assistant, see Section 2.6, "Upgrading Schemas Using Patch Set Assistant".

18.7 Upgrading Oracle Platform Security Services on OESHOST1

After you upgrade Oracle Platform Security Services schema on `OESHOST1`, you must upgrade Oracle Platform Security Services (OPSS) on `OESHOST1`. This task is optional; however, it is recommended that you perform this task.

> **Note:** If you are upgrading Oracle Entitlements Server 11.1.2.1.0 environments to 11.1.2.2.0, you must upgrade Oracle Platform Security Services if Audit schema is installed. This step is required to upgrade the policy store to include the new 11.1.2.2.0 audit policies.

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Entitlements Server to 11.1.2.2.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see Section 2.7, "Upgrading Oracle Platform Security Services".

18.8 Updating Binaries of WebLogic Server and Access Manager on OESHOST2

After upgrading Oracle Platform Security Services on `OESHOST2`, you must update the binaries of Oracle WebLogic Server and Oracle Entitlements Server to 10.3.6 and 11.1.2.2.0 versions respectively on `OESHOST2` by completing the following tasks:

1. Updating Oracle WebLogic Server Binaries to 10.3.6
2. Updating Oracle Entitlements Server Binaries to 11.1.2.2.0

18.8.1 Updating Oracle WebLogic Server Binaries to 10.3.6

Oracle Identity and Access Management 11.1.2.2.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Identity Manager environment is using Oracle WebLogic Server 10.3.5 or the previous versions, you must update the Oracle WebLogic Server binaries to 10.3.6 by completing the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

   For more information, see "Downloading an Upgrade Installer From My Oracle Support" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

   For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

18.8.2 Updating Oracle Entitlements Server Binaries to 11.1.2.2.0

To update the existing Oracle Entitlements Server binaries to Oracle Entitlements Server 11.1.2.2.0, you must use the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Installer. During the procedure, specify the location of your existing Middleware Home. This updates the Oracle Entitlements Server binaries 11.1.2.2.0.

For information about updating Oracle Entitlements Server binaries to 11.1.2.2.0, see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

18.9 Redeploying APM Applications on OESHOST1 and OESHOST2

After you update Oracle Entitlements Server binaries on `OESHOST2`, you must redeploy the following APM applications on `OESHOST1` and `OESHOST2`:

- `oracle.security.apm.ear`
- `oracle.security.apm.core.model.ear`
- `oracle.security.apm.core.view.war`

To redeploy the APM applications, do the following:

1. Start the Weblogic Administration Server. For more information, see Section 2.9.2, "Starting the WebLogic Administration Server".
2. Launch the WebLogic Scripting Tool (WLST) by running the commnad from the location *$MWHOME*`/wlserver_10.3/common/bin`:

   On UNIX: `./wlst.sh`

   On Windows: `wlst.cmd`
3. Connect to the Administration Server by running the following command:

   `connect('`*weblogic-username*`','`*weblogic-password*`','`*weblogic-url*`')`
4. Run the following commands to redeploy the APM applications:

   On UNIX:

   - `redeploy(appName='oracle.security.apm')`
   - `redeploy(appName='oracle.security.apm.core.model')`
   - `redeploy(appName='oracle.security.apm.core.view')`

   On Windows:

   - *$DOMAIN_HOME*`\serverConfig\redeploy(appName='oracle.security.apm')`
   - *$DOMAIN_HOME*`\serverConfig\redeploy(appName='oracle.security.apm.core.model')`
   - *$DOMAIN_HOME*`\serverConfig\redeploy(appName='oracle.security.apm.core.view')`

   In these commands, *$DOMAIN_HOME* refers to the absolute path to the Oracle Entitlements Server 11.1.2.2.0 domain.

   The following is an example of redeploying an APM application on Windows:

   ```
   C:\Oracle\Middleware\user_projects\domains\OES_Domain\serverConfig\
   redeploy(appName='oracle.security.apm')
   ```
5. Stop the WebLogic Administration Server. For more information, see Section 2.9.2, "Starting the WebLogic Administration Server".

18.10 Starting Administration Server and Managed Servers on OESHOST1 and OESHOST2

Start the WebLogic Administration Server and the Oracle Entitlements Server Managed Servers on `OESHOST1` and `OESHOST2` in the following order:

1. Start the WebLogic Administration Server on `OESHOST1`.
2. Start the Oracle Entitlements Server Managed Servers on `OESHOST1` and `OESHOST2`.

For more information about starting the WebLogic Administration Server, see Section 2.9.2, "Starting the WebLogic Administration Server".

For more information about starting the Managed Servers, see Section 2.9.3, "Starting the Managed Server(s)".

19

Upgrading Oracle Privileged Account Manager High Availability Environments

This chapter describes how to upgrade Oracle Privileged Account Manager high availability environments to 11*g* Release 2 (11.1.2.2.0) on Oracle WebLogic Server.

> **Note:** Before proceeding, check if your existing Oracle Privileged Account Manager version is supported for high availability upgrade. For more information on supported starting points for high availability upgrade, see Section 1.5, "Supported Starting Points for Upgrading High Availability Environments".

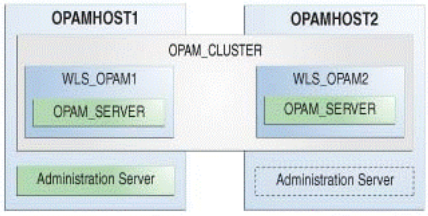
This chapter includes the following sections:

- Section 19.1, "Understanding Oracle Privileged Account Manager High Availability Upgrade Topology"
- Section 19.2, "Upgrade Roadmap"
- Section 19.3, "Shutting Down all Servers on OPAMHOST1 and OPAMHOST2"
- Section 19.4, "Backing Up the Existing Environment"
- Section 19.5, "Updating Binaries of WebLogic Server and Oracle Privileged Account Manager on OPAMHOST1 and OPAMHOST2"
- Section 19.6, "Upgrading Database Schemas on OPAMHOST1"
- Section 19.7, "Starting Administration Server, Node Manager, and Managed Servers on OPAMHOST1 and OPAMHOST2"
- Section 19.8, "Redeploying Applications on OPAMHOST1"
- Section 19.9, "Verifying the Domain Upgrade"
- Section 19.10, "Optional: Configuring Oracle Privileged Account Manager Session Manager"
- Section 19.11, "Optional: Configuring Oracle Identity Navigator for WLS_OPAM1 and WLS_OPAM2"

19.1 Understanding Oracle Privileged Account Manager High Availability Upgrade Topology

Figure 19–1 shows the Oracle Privileged Account Manager cluster set up that can be upgraded to 11.1.2.2.0 by following the procedure described in this chapter.

Figure 19–1 Oracle Privileged Account Manager High Availability Upgrade Topology



The host OPAMMHOST1 has the following installations:

- An Oracle Privileged Account Manager instance in the WLS_OPAM1 Managed Server.
- A WebLogic Server Administration Server. Under normal operations, this is the active Administration Server.

The host OPAMMHOST2 has the following installations:

- An Oracle Privileged Account Manager instance in the WLS_OPAM2 Managed Server.
- A WebLogic Server Administration Server. Under normal operations, this is the passive Administration Server. You make this Administration Server active if the Administration Server on OPAMHOST1 becomes unavailable.

The instances in the WLS_OPAM1 and WLS_OPAM2 Managed Servers on OPAMHOST1 and OPAMHOST2 are configured as the cluster named OPAM_CLUSTER.

19.2 Upgrade Roadmap

Table 19–1 lists the steps to upgrade Oracle Privileged Account Manager high availability environment illustrated in Figure 19–1 to 11.1.2.2.0.

Table 19–1 Oracle Privileged Account Manager High Availability Upgrade Roadmap

Task No	Task	For More Information
1	Review the Oracle Privileged Account Manager high availability upgrade topology, and identify OPAMHOST1 and OPAMHOST2 on your setup.	See, Understanding Oracle Privileged Account Manager High Availability Upgrade Topology
2	Shut down the Administration Server, Oracle Privileged Account Manager Managed Servers, and the Node Manager on OPAMHOST1 and OPAMHOST2.	See, Shutting Down all Servers on OPAMHOST1 and OPAMHOST2
3	Back up the Middleware Home, the Oracle Home, and the Database schemas on OPAMHOST1 and OPAMHOST2.	See, Backing Up the Existing Environment
4	Update the binaries of WebLogic Server and Oracle Privileged Account Manager on OPAMHOST1 and OPAMHOST2.	See, Updating Binaries of WebLogic Server and Oracle Privileged Account Manager on OPAMHOST1 and OPAMHOST2
5	Upgrade the OPAM and OPSS schema on OPAMHOST1 by running the Patch Set Assistant.	See, Upgrading Database Schemas on OPAMHOST1

Table 19–1 (Cont.) Oracle Privileged Account Manager High Availability Upgrade

Task No	Task	For More Information
6	Start the WebLogic Administration Server and all the Managed Servers on `OPAMHOST1` and `OPAMHOST2`.	See, Starting Administration Server, Node Manager, and Managed Servers on OPAMHOST1 and OPAMHOST2
7	Redeploy the Oracle Identity Navigator application `oinav.ear` and Oracle Privileged Account Manager application `opam.ear` on `OPAMHOST1`.	See, Redeploying Applications on OPAMHOST1
8	Verify the domain upgrade.	See, Verifying the Domain Upgrade
9	If you wish to configure Oracle Privileged Account Manager session manager which is newly introduced in 11.1.2.2.0, you can do so by running the WLST command `configureSessionManager.py`, and targeting it to the `OPAM_CLUSTER`. This step is optional.	See, Optional: Configuring Oracle Privileged Account Manager Session Manager
10	If you wish to configure Oracle Identity Navigator for the Oracle Privileged Account Manager Managed Servers `WLS_OPAM1` and `WLS_OPAM2`, you can do so by running the configuration wizard on `OPAMHOST1`. This step is optional.	See, Optional: Configuring Oracle Identity Navigator for WLS_OPAM1 and WLS_OPAM2

19.3 Shutting Down all Servers on OPAMHOST1 and OPAMHOST2

Before you begin the upgrade process, you must stop the WebLogic Administration Server, Oracle Privileged Account Manager Managed Servers, and Node Manager on `OPAMHOST1` and `OPAMHOST2` in the following order:

1. Stop the Oracle Privileged Account Manager Managed Servers on both `OPAMHOST1` and `OPAMHOST2`.
2. Stop the WebLogic Administration Server on `OPAMHOST1`.
3. Stop the Node Manager on `OPAMHOST1` and `OPAMHOST2`.

For information about stopping the Managed Server, see Section 2.8.1, "Stopping the Managed Server(s)".

For information about stopping the Administration Server, see Section 2.8.2, "Stopping the WebLogic Administration Server".

For information about stopping the Node Manager, see Section 2.8.3, "Stopping the Node Manager".

19.4 Backing Up the Existing Environment

After stopping all the servers, you must back up the following before proceeding with the upgrade process:

- *MW_HOME* directory (Middleware home directory), including the Oracle Home directories inside Middleware home on both `OPAMHOST1` and `OPAMHOST2`.

- Oracle Privileged Account Manager Domain Home directory on both `OPAMHOST1` and `OPAMHOST2`.
- Following Database schemas:
  - Oracle Privileged Account Manager schema
  - Oracle Platform Security Services schema

  For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

19.5 Updating Binaries of WebLogic Server and Oracle Privileged Account Manager on OPAMHOST1 and OPAMHOST2

After You must update the binaries of Oracle WebLogic Server and Oracle Privileged Account Manager to 10.3.6 and 11.1.2.2.0 versions respectively on `OPAMHOST1` and `OPAMHOST2` by completing the following tasks:

1. Updating Oracle WebLogic Server Binaries to 10.3.6 on OPAMHOST1 and OPAMHOST2
2. Updating Oracle Privileged Account Manager Binaries to 11.1.2.2.0 on OPAMHOST1 and OPAMHOST2

19.5.1 Updating Oracle WebLogic Server Binaries to 10.3.6 on OPAMHOST1 and OPAMHOST2

Oracle Identity and Access Management 11.1.2.2.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Identity Manager environment is using Oracle WebLogic Server 10.3.5 or the previous versions, you must update the Oracle WebLogic Server binaries to 10.3.6 by completing the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

   For more information, see "Downloading an Upgrade Installer From My Oracle Support" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

   For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

19.5.2 Updating Oracle Privileged Account Manager Binaries to 11.1.2.2.0 on OPAMHOST1 and OPAMHOST2

To update the existing Oracle Privileged Account Manager binaries to Oracle Privileged Account Manager 11.1.2.2.0, you must use the Oracle Identity and Access Management 11*g* Release 2 (11.1.2.2.0) Installer. During the procedure, specify the location of your existing Middleware Home. This upgrades the Oracle Privileged Account Manager binaries to 11.1.2.2.0.

For information about updating Oracle Privileged Account Manager binaries to 11.1.2.2.0, see Section 2.4, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.2.0)".

19.6 Upgrading Database Schemas on OPAMHOST1

On `OPAMHOST1`, you must upgrade the following schemas by running the Patch Set Assistant:

- OPAM schema
- OPSS schema - OPSS schema is selected as a dependency when you select OPAM.

For information about upgrading schemas using Patch Set Assistant, see Section 2.6, "Upgrading Schemas Using Patch Set Assistant".

After you upgrade the OPAM and OPSS schemas, the version of the OPAM schema will be 11.1.2.2.0.

19.7 Starting Administration Server, Node Manager, and Managed Servers on OPAMHOST1 and OPAMHOST2

After upgrading the database schemas on `OPAMHOST1`, you must start the WebLogic Administration Server, Node Manager, and the Oracle Privileged Account Manager Managed Servers on `OPAMHOST1` and `OPAMHOST2` in the following order:

1. On `OPAMHOST1`. start the WebLogic Administration Server, Node Manager, and Oracle Privileged Account Manager Managed Server.
2. On `OPAMHOST2`, start the Node Manager, and the Oracle Privileged Account Manager Managed Server.

For more information about starting the WebLogic Administration Server, see Section 2.9.2, "Starting the WebLogic Administration Server".

For more information about starting the Node Manager, see Section 2.9.1, "Starting the Node Manager".

For more information about starting the Managed Servers, see Section 2.9.3, "Starting the Managed Server(s)".

19.8 Redeploying Applications on OPAMHOST1

After you start the servers, you must redeploy Oracle Identity Navigator and Oracle Privileged Account Manager applications on `OPAMHOST1` namely `oinav.ear` and `opam.ear`. You can do this using either the WebLogic Administration console or the WebLogic Scripting Tool (WLST).

For more information about redeploying Oracle Identity Navigator and Oracle Privileged Account Manager applications, see Section 7.9, "Redeploying the Applications".

19.9 Verifying the Domain Upgrade

Verify that the Oracle Privileged Account Manager domain was upgraded successfully by doing the following:

1. Log in to the Oracle Privileged Account Manager 11.1.2.2.0 console using the following URL:

   `http://`*`adminserver_host`*`:`*`adminserver_port`*`/oinav/opam`

2. Verify that the pre-upgrade data, targets, accounts, grants are present, and working as expected.

19.10 Optional: Configuring Oracle Privileged Account Manager Session Manager

The Oracle Privileged Account Manager session manager application named `opamsessionmgr` is introduced in 11.1.2.2.0. If you wish to configure the Oracle Privileged Account Manager session manager application, you must run the WebLogic Scripting Tool (WLST) command `configureSessionManager.py` on `OPAMHOST1`, and target it to the `OPAM_CLUSTER`.

For more information about configuring Oracle Privileged Account Manager session manager, see Section 7.13, "Optional: Configuring the Oracle Privileged Account Manager 11.1.2.2.0 Session Manager".

After you configure Oracle Privileged Account Manager session manager, start all the servers on `OPAMHOST1` and `OPAMHOST2`. For more information about starting all the servers, see Starting Administration Server, Node Manager, and Managed Servers on OPAMHOST1 and OPAMHOST2.

19.11 Optional: Configuring Oracle Identity Navigator for WLS_OPAM1 and WLS_OPAM2

If you wish to configure Oracle Identity Navigator that hosts Oracle Privileged Account Manager console, to run on the Oracle Privileged Account Manager Managed Servers `WLS_OPAM1` and `WLS_OPAM2` in order to achieve high availability use cases for the Oracle Privileged Account Manager console, complete the steps described in Section 7.14, "Optional: Configuring Oracle Identity Navigator Application on OPAM Managed Server".

After configuring Oracle Identity Navigator successfully, you can access Oracle Identity Navigator on `WLS_OPAM1` and `WLS_OPAM2` at the non-SSL port using the following URL:

`http://`*`opamserver_host`*`:`*`opamserver_nonssl_port`*`/oinav/opam`

The default non-SSL port is `18101`. Oracle Identity Navigator will still run on the WebLogic Administration Server. After you configure Oracle Identity Navigator for Oracle Privileged Account Manager Managed Server, you must update the Oracle HTTP Server configuration for Oracle Identity Navigator on `OPAMHOST1`, to achieve high availability. For more information, see "Update the Oracle HTTP Server Configuration" in the *Oracle Fusion Middleware High Availability Guide*.

After you configure Oracle Identity Navigator for Oracle Privileged Account Manager Managed Servers, start all the servers on `OPAMHOST1` and `OPAMHOST2`. For more information about starting all the servers, see Starting Administration Server, Node Manager, and Managed Servers on OPAMHOST1 and OPAMHOST2.